FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Financial Institutions' Use of Information
and Communications Technology (ICT)

RISK AND VULNERABILITY ANALYSIS
2022

CONTENTS

1 SUMMARY 3
2 FINANCIAL INFRASTRUCTURE 7
2.1 The importance of the financial infrastructure 7
2.2 Financial Infrastructure Crisis Preparedness Committee (BFI) 9
2.3 Cooperation in the area of security 9
2.4 Changes in the financial infrastructure and joint efforts by the financial industry 11
3 FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS 14
3.1 The financial infrastructure is robust 14
3.2 An evolving cyberthreat picture 15
3.3 The Covid-19 pandemic and the war in Ukraine 19
3.4 Supervision of ICT and payment services 19
3.5 Account servicing payment service provider PSD2 interfaces 22
3.6 Institutions' assessments of risk and vulnerability 23
3.7 Risk associated with customers' use of digital services 30
3.8 Risk associated with vulnerabilities in institutions' ICT operations 32
4 FRAUD AND FRAUD STATISTICS 34
4.1 Reporting of fraud statistics 34
4.2 Losses associated with the fraudulent use of payment cards 34
4.3 Losses linked to account transfers 37
4.4 Losses from social engineering fraud 37
4.5 Losses from fraud where the fraudster issues the payment order 38
5 INCIDENT REPORTING 39
5.1 Incident statistics 39
5.2 Security incidents 40
5.3 Reporting vulnerabilities 40
5.4 Security breaches 41
5.5 Operational incidents 41
5.6 Analysis of incidents as a measure of availability 44
5.7 Incidents related to problems with dedicated PSD2 interfaces 46
6 OUTSOURCING 47
6.1 Outsourcing notifications 47
6.2 Regulatory changes and guidelines on outsourcing 48
6.3 Management and control 48

6.4 Risk associated with outsourcing 49

APPENDIX 1: THE INSTITUTIONS' ASSESSMENT OF VULNERABILITY 53

APPENDIX 2: BASIS FOR THE RISK MATRIX 61

APPENDIX 3: FINANSTILSYNET'S MONITORING ACTIVITIES.....70

APPENDIX 4: GUIDELINES FROM EBA, EIOPA AND ESMA 74

APPENDIX 5: MAPPING OF BUSINESS-CRITICAL ASSETS, SOFTWARE, BUSINESS FUNCTIONS, PROCESSES AND INFORMATION 75

1 Summary

Norway's financial infrastructure is robust. At the same time, the threat picture is constantly evolving. During the Covid-19 pandemic and in connection with the war in Ukraine, Finanstilsynet and the Financial Infrastructure Crisis Preparedness Committee (BFI) have paid particular attention to entities that support important functions, including critical social functions identified by the Norwegian Directorate for Civil Protection (DSB).[1] The key institutions in Norway's financial infrastructure generally have good contingency plans. The actors have maintained control over the operational situation and have quickly implemented the required measures.

No ICT incidents impacted financial stability in 2021. The number of security incidents was approximately the same as in 2020 and lower than in 2019, while there were significantly more operational incidents. Overall, the number of reported ICT incidents rose by more than 40 per cent, to 292. Given the duration of the incidents, the number of users affected and at what time of day they occurred, Finanstilsynet's assessment is that the overall availability of payment and other customer services in 2021 was better than in the preceding years.

The scale of cybercrime in 2021 appears to have been on a par with that in 2020. However, incidents that occurred in 2021 revealed serious vulnerabilities in some institutions. Attempts to exploit vulnerabilities were observed, although the attackers failed to gain access to the institution's IT systems. So far, no cybercrime targeted at institutions in the Norwegian financial sector has had serious consequences.

The institutions are continuously fortifying their defences. The financial sector's cooperation via NFCERT[2] is helping to improve knowledge about the relevant threat and risk picture, and better equip the institutions to handle cyberthreats and adverse incidents.

In recent years, incidents after changing operations service providers have shown that principals must get better at quality assuring that service providers have adequate procedures, expertise and capacity to effectively deal with serious incidents that impact critical services.

Through its supervisory activities, Finanstilsynet uncovered vulnerabilities that represent a risk of serious incidents in the financial services sector. For example, Finanstilsynet has identified weaknesses in institutions' work on business continuity and contingency plans. Furthermore, Finanstilsynet has

[1] BFI is chaired by Finanstilsynet and follows up preparedness and incidents in the financial infrastructure. The link points to the topic page on Finanstilsynet's website.
[2] Nordic Financial CERT The link points to NFCERT's website.

pointed out omissions in the documentation of institutions' own ICT infrastructure and omissions in the monitoring of service providers. Weaknesses have also been identified in security work, including in monitoring service providers' access to institutions' systems and data.

Merger processes, which are often demanding and time-consuming, should include unified testing strategies with clear divisions of responsibility. The testing should be based on established acceptance criteria and cover different types of customers, products and services, as well as internal production and oversight processes. High levels of emergency preparedness and call centre capacity are also important when mergers are carried out.

Finanstilsynet believes that in order to ensure the resilience of the financial infrastructure, institutions should improve their ICT efforts, both to reduce the likelihood of operational incidents and to enhance ICT security. There must be a strong focus on developments in the cyberthreat picture.

In 2021, emergency preparedness in the electronic payment system was strengthened by significantly increasing the capacity of the backup solution in payment terminals when using BankAxept payment cards.

Finanstilsynet considers vulnerabilities in institutions' defences against cybercrime to be the main ICT risk, where the overall risk and probability are considered high and the consequences serious. Vulnerabilities in relation to ICT operations, access management and information leaks are also key risks, and the overall risk is considered moderate to high. While the risk associated with institutions' defences against cybercrime and access management was regarded as marginally higher in 2021, the risk associated with ICT operations is regarded as slightly lower.

The institutions' assessments of operational risk and security risk, as stated in their reporting and dialogue with Finanstilsynet, show that the threat from cybercrime has increased, attack surfaces have increased in number, and several institutions have registered a higher number of attacks. A need for further ICT security measures, training and increased resources has been identified. Monitoring of business-critical hardware, software, business functions, procedures and information is challenging but important when it comes to maintaining oversight of ICT and security risks, and it is also important to have sufficient insight into the security architecture of one's own and service providers' ICT services. It is also clear that, as in previous years, recruiting employees with expertise in information security and monitoring of outsourced activities is challenging, and that there is an increased risk associated with new regulations that entails a need for changes to ICT systems.

Digitalisation is providing customers with new, and often better, services at a lower cost. At the same time, it is creating new risks, both for service providers and for their customers. The failure of some merchants to use strong customer authentication (SCA) for e-commerce exposes cardholders to a risk of fraud.

The large-scale use of BankID for both private and public services with variations in login text, entails a risk of users not being sufficiently vigilant and being tricked into fake logins. Nor can users opt out of areas of use and reduce the potential for misuse. To reduce the risk of fraud, service providers are using so-called backend testing in the form of transaction and customer analytics as part of approval processes for logins and for initiating transactions.

The misuse of ID characteristics is also an area of risk. To reduce the risk of fraud through the misuse of ID characteristics, the Norwegian Data Protection Authority recommends that users actively block credit ratings at credit rating agencies.[3] Today, activating such blocks is demanding for the consumer since they have to contact each credit rating agency individually to activate the block. The Norwegian Data Protection Authority has taken the initiative to develop a common blocking solution via the Brønnøysund Register Centre.

The financial sector is working on an ongoing project to develop and implement measures aimed at securing the use of digital banking services in order to help reduce the likelihood of fraud occurring and mitigate the consequences of fraud.

Some 147,000 fraudulent transactions were carried out with cards in 2021, compared with 205,000 in 2020. Despite the drop in the number of fraudulent transactions, losses from card fraud increased by 9.9 per cent to NOK 162 million in 2021. The proportion of fraudulent transactions was highest for cross-border transactions. The proportion for all transactions was 0.006 per cent, while it was 0.2 per cent for transactions carried out in countries outside the EEA. For card payments initiated non-electronically, the proportion of fraudulent transactions was 0.24 per cent in 2021.

Losses due to account transfers, mainly using online banks, amounted to NOK 346 million in 2021, which was 2.5 per cent lower than the year before. The losses related to both transactions in which the fraudster issued or modified the payment, and transactions where the fraudster manipulated the payer into making the payment themselves.

Losses due to social engineering, i.e. where the payer is tricked into carrying out the fraudulent transaction, amounted to NOK 240.6 million in 2021. Of this, NOK 224 million stemmed from account transfers and NOK 16.6 million from payment card use. Even though the number of attempted scams is steadily increasing, the amount lost in 2021 was lower than in 2020, when social engineering losses amounted to NOK 295 million. One important reason for the decrease is probably that banks are preventing an ever larger proportion of attempted scams. Social engineering fraud still appears to be the most profitable method for criminals.

Institutions are responsible for all of their ICT operations, including when some of them have been outsourced. Institutions must assess a number of risk factors when considering outsourcing, including

[3] The Norwegian Data Protection Authority's webpage on credit ratings, including on blocking credit rating at credit rating agencies (in Norwegian only).

management and control, monitoring of service providers, security and business continuity and emergency preparedness. Practically all institutions supervised by Finanstilsynet have entered into agreements that outsource parts of their ICT operations.

In 2021, Finanstilsynet received more than 170 outsourcing notifications. Finanstilsynet specifically followed up the banks' plans for emergency preparedness when Vipps changed its BankID operations service provider.

As in previous years, the outsourcing notifications bear testimony to the growing use of cloud services for both application and infrastructure services. Institutions often end up having to deal with a larger number of platforms. More platforms result in greater complexity and a more complicated risk picture.

In Finanstilsynet's opinion, the quality of the institutions' analyses and assessments of risk prior to implementing ICT outsourcing has improved. The quality of agreements with service providers and management's understanding of the institution's outsourcing agreements also show a positive development. Some institutions, however, need to improve their work on outsourcing.

The main themes for Finanstilsynet's supervisory activities in relation to ICT and payment services in 2022 will be the institutions' management and control of ICT operations, their work on security surrounding their ICT solutions, including cybersecurity, and their preparedness work and testing of business continuity and disaster recovery solutions. Furthermore, through its supervisory activities, Finanstilsynet will assess management, control and monitoring of outsourced ICT operations, institutions' payment services and major changes in the financial infrastructure.

Finanstilsynet will continue to monitor ICT incidents and vulnerabilities in institutions' ICT solutions. The emphasis will be on institutions identifying causes and implementing preventive measures. The threat picture for cybercrime is monitored and institutions' preparedness work targeting cyber vulnerability and cybersecurity is reviewed.

Finanstilsynet believes it is important that institutions properly address the security of their services so that customers do not suffer losses. Through its supervisory activities, Finanstilsynet also ensures that institutions do not share their customers' data without consent and that these data do not fall into the hands of unauthorised parties.

BFI follows up preparedness and incidents in the financial infrastructure. In special circumstances, such as the Covid-19 pandemic and the war in Ukraine, BFI will monitor the ICT operations and emergency preparedness of the most important actors especially closely.

For further information about Finanstilsynet's monitoring of supervised institutions, see appendix 3.

2 FINANCIAL INFRASTRUCTURE

2.1 The importance of the financial infrastructure

Effective, robust, and stable payment systems are a prerequisite for financial stability and well-functioning markets. The financial infrastructure is designed to ensure that payments and transactions in financial instruments are registered, cleared and settled.

Failures by key actors in the financial industry or in the infrastructure can have significant social consequences.[4] The financial infrastructure is complex, intricate and includes many actors and service providers. Poor resilience or security at a single actor or service provider can constitute a weak link in the overall value chains and incidents can spill over to other actors. The Norwegian Directorate for Civil Protection (DSB) has identified financial services as a critical social function.[5] The Ministry of Justice and Public Security has tasked DSB with revising the listing of critical social functions on an ongoing basis. Finanstilsynet has provided input.

If payments or securities trades cannot be executed or settled, important social functions will quickly stop working satisfactorily. Sensitive information going astray or breaches of the rules for processing inside information may undermine confidence in marketplaces and the financial system. If unauthorised persons gain access to customer and account data and compromise them or render them unavailable, customers and institutions can face significant challenges. The social consequences could be particularly severe if institutions operating on behalf of many or all institutions are affected. The financial sector is also dependent on infrastructure such as power supplies and telecommunications.

Finanstilsynet and Norges Bank cooperate on the supervision and surveillance of the financial infrastructure in Norway, including through reports, risk assessments and joint supervision.

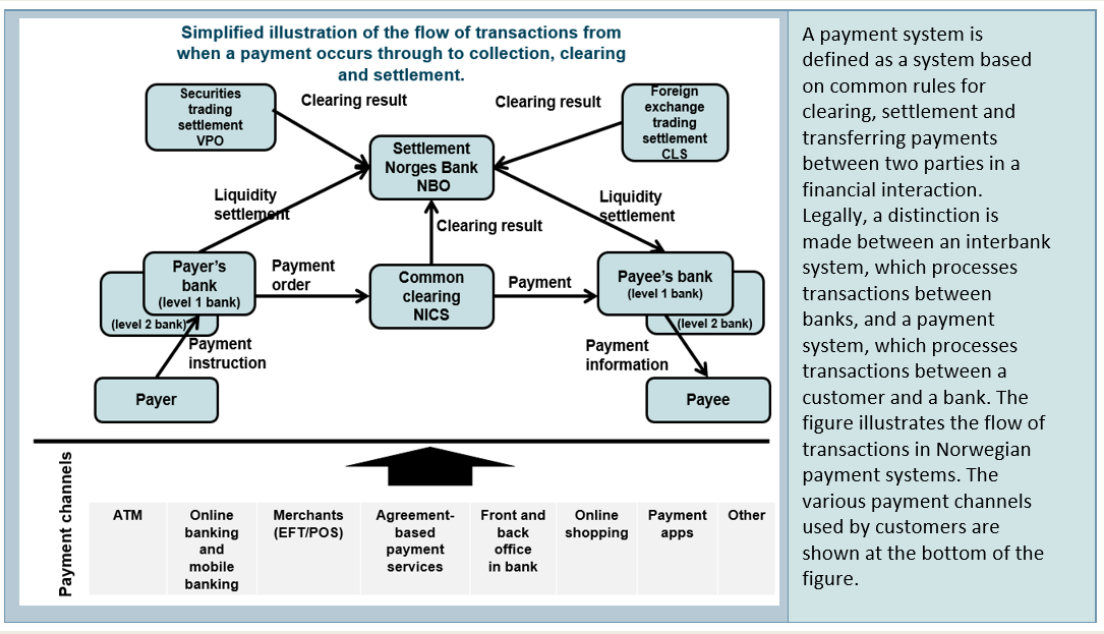
[4] The Security Act defines both economic stability and freedom of action as national security interests, cf. Security Act, section 1-5 Definitions (Lovdata). This includes financial infrastructure and objects that are vital to the functioning of civil society.
[5] Norwegian Directorate for Civil Protection (DSB): Vital functions in society

Flows of transactions in the Norwegian payment system

The financial infrastructure consists of the payment system and the securities settlement system, as well as the Norwegian Central Securities Depository, marketplaces and key counterparties.

The payment system includes interbank systems and systems for payment services for transferring funds, with formal and standardised arrangements and common rules for processing, clearing, or settling payment transactions.

The payment system, including payment services, is regulated by legislation such as the Act relating to Payment Systems, Regulations on Payment Services Systems, and Regulations on Payment Services, as well as through the financial services sector's self-regulation administered by Finance Norway and Bits.



A payment system is defined as a system based on common rules for clearing, settlement and transferring payments between two parties in a financial interaction. Legally, a distinction is made between an interbank system, which processes transactions between banks, and a payment system, which processes transactions between a customer and a bank. The figure illustrates the flow of transactions in Norwegian payment systems. The various payment channels used by customers are shown at the bottom of the figure.

Source: Finanstilsynet

The securities sector is regulated by legislation such as the Securities Trading Act, the Securities Trading Regulations and the Central Securities Depository Act. The securities sector includes actors involved in securities transactions related to equity instruments such as shares and equity certificates, including the execution of trades and related settlements.

2.2 Financial Infrastructure Crisis Preparedness Committee (BFI)

The Financial Infrastructure Crisis Preparedness Committee (BFI) was established in order to:

- prepare and coordinate measures for preventing and resolving crisis situations and other situations that may result in major disruptions to the financial infrastructure. In a crisis situation, the committee must notify and inform affected entities and authorities of the problems that have occurred, the potential consequences of the problems and the measures that must be implemented to resolve the problems.
- perform the necessary coordination of preparedness matters within the financial services sector. This includes, based on the civil preparedness system, coordinating the preparation and implementation of notification plans and preparedness measures in the event of national security policy crises and war.

Finanstilsynet chairs and is the secretariat for the committee. Central authorities and actors in the financial infrastructure sit on the committee. BFI holds regular meetings and conducts annual emergency response exercises. The work in BFI, which reviews severe and critical incidents, helps provide Finanstilsynet with a good, broad picture of the status of the financial infrastructure. Further information is available on Finanstilsynet's website on the webpage about the Financial Infrastructure Crisis Preparedness Committee (BFI).

2.3 Cooperation in the area of security

Entities with critical social functions in the financial services sector

The Security Act[6] defines economic stability and freedom of action as one of a number of national security interests[4] that must be monitored by the responsible sectoral ministry. Ministries must identify and maintain an overview of entities that are of vital or material importance to fundamental national functions (FNFs) and report these to the Norwegian National Security Authority (NSM). As far as institutions of vital importance to FNFs in the financial sector are concerned, it is the Ministry of Finance that decides whether an institution should be fully or partially subject to the Security Act. The ministry has made decisions in relation to some private actors, but not within the Finanstilsynet's area of responsibility. This work has not been completed.

Institutions of vital or material importance to an FNF may be more attractive targets for attacks by foreign intelligence services. Threats from foreign state actors are described in section 3.2.2.

Cooperation and information sharing result in a better understanding of risk

Cooperation and information sharing between financial institutions in Norway via Nordic Financial CERT (NFCERT)[2] help improve knowledge about the relevant threat and risk picture,

[6] Lovdata: Act relating to national security (Security Act)

and better equip the institutions to handle cyberthreats and adverse incidents. NFCERT prepares regular threat reports. In Finanstilsynet's experience, institutions that do not take part in this partnership may be poorly equipped to manage cyberthreats and adverse incidents.

Finanstilsynet has been designated as sectoral response environment (SRE)[7] by the Ministry of Finance and tasked with handling ICT security incidents in that part of the financial services sector for which Finanstilsynet is responsible. Finanstilsynet performs this role in cooperation with NFCERT.

Finanstilsynet participates as a partner in the Norwegian National Cybersecurity Centre (NCSC), which was established by the Norwegian National Security Authority (NSM) to strengthen the country's cyber resilience and preparedness. Participation provides Finanstilsynet with access to up-to-date knowledge of the risk picture in the area of cybersecurity, as well as the ability to interact and exchange information with other actors in dealing with cyberthreats and cyberattacks. Finanstilsynet also participates in the NSM's SIG[8] ICT, which is a cooperative forum for authorities that supervise ICT security in their sector.

Finanstilsynet and Norges Bank established the TIBER-NO[9] framework for testing cybersecurity in the financial sector in 2021. Forums have also been established that facilitate overarching follow-up, management and the involvement of industry actors and other relevant authorities. The purpose behind TIBER-NO is to promote financial stability through increasing the resilience of critical functions in the Norwegian financial system against cyberattacks. See section 3.2.5 for further information.

European cooperation and information exchange

In January 2022, the European Systemic Risk Board (ESRB) published a strategy for reducing the risk of financial instability as a result of cyber incidents.[10] For instance, a need to develop means of macro regulation that capture systemic cyber risk has been identified. The ESRB also recommends that a European framework be established for coordination in the event of systemic cyber incidents (EU-SCICF), cf. the provision on cross-sectoral cooperation in the proposal for a regulation on digital operational resilience for the financial sector (DORA).[11] The purpose is to ensure rapid communication and coordination between supervisory authorities and with other relevant authorities in order to avoid coordination failures in the event of a serious incident occurring.

[7] The Norwegian National Security Authority (NSM): Rammeverk for håndtering av IKT-hendelser (in Norwegian only)
[8] SIG stands for special interest group
[9] TIBER stands for 'Threat Intelligence-based Ethical Red Teaming', see Finanstilsynet's news item dated 21 October 2021: Norges Bank og Finanstilsynet etablerer rammeverk for testing av cybersikkerhet i finansiell sektor (TIBER-NO) (in Norwegian only)
[10] European Systemic Risk Board (ESRB): Mitigating systemic cyber risk (January 2022)
[11] EU's proposal for a regulation on digital operational resilience: Digital Operational Resilience Act. Also see the discussion in RVA 2021

2.4 Changes in the financial infrastructure and joint efforts by the financial industry

A number of significant changes were announced and implemented in the Norwegian financial infrastructure in 2021. Some of the planned changes will be implemented in 2022, others in 2023–2024.

In 2021, Mastercard decided to take over operation of the banks' payment services, the Norwegian Interbank Clearing System (NICS) and the common operational infrastructure (FOI services)[12]. Nets has assisted Mastercard in operating the solutions following the transfer of Nets' account-to-account services to Mastercard in 2021. The transfer is expected to start in 2022 and be completed in 2024.

Vipps AS changed its operations service provider for BankID in October 2021. The change of service provider from Nets to DXC resulted in significant capacity challenges, especially for ordinary (bank held) BankID. BankID on mobile phones was not particularly affected, see section 5.5.

The common operational infrastructure for instant payments ('Straks FOI') was established in 2013 and the solution has gradually been adopted by most banks. The solution is now being further developed as part of the modernisation project associated with NICS, where the message format for submission will be changed from NISOK/NIBE to ISO 20022 format. In 2022, after migration to ISO 20022, the banks will send their instant payments directly to the NICS Real clearing solution. Once all the banks have migrated to the new messaging format and to NICS Real, 'Straks FOI' from 2013 will be phased out.

Norges Bank assists banks in settling transactions via the NBO settlement function. In June 2021, Norges Bank circulated for consultation a study on the central bank's role as a settlement bank when introducing instant payments including for the settlement of interbank transactions. Norges Bank outlined two alternative solutions:

1) acquiring and establishing a separate system for the settlement of instant payments in Norges Bank
2) cooperating with other central banks in Europe through connection to the Eurosystem's TIPS solution[13]

Banks, banking alliances and key service providers in Norway all submitted their views in the consultation process. In autumn 2021, Norges Bank decided to commence negotiations with the ECB

[12] The common operational infrastructure includes areas where the banking industry has, in joint agreements under the auspices of the principal, stipulated that all banks must use the deliveries of one operational unit to implement specific payment services and/or information exchange transactions such as BankAxept, BankID and several of the banks' payment services, including AvtaleGiro and eInvoice. See Rammeavtale om utvikling, forvaltning og drift av felles operasjonell infrastruktur (FOI) (in Norwegian only).
[13] Target Instant Payment System (TIPS) – Eurosystem's infrastructure for instant payments

on participation in the Eurosystem's TIPS solution.[14] The changes resulting from Norges Bank's decision could have a significant impact on the payment system and services in Norway.

In 2020, the Eika Alliance entered into an agreement with Tietoevry regarding delivery of core banking solutions to the local banks in the alliance. The transition from SDC to Tietoevry is scheduled for completion in 2022-2023. The agreement will result in the proportion of Norwegian banks using Tietoevry as their operations service provider increasing significantly in the financial sector. This will result in increased concentration risk.

In order to deliver better cross-border services in the Nordic countries, Vipps entered into an agreement in 2021 for a common solution for Vipps' wallet and payment solutions, Danske Bank's wallet Mobilpay and OP Financial Group's wallet Pivo. Implementation will require permission from authorities in several countries. The agreement also means that BankAxept and BankID will be separated from the wallet business in Vipps and established as their own company.

Improved emergency preparedness in the electronic payment system

In 2021, emergency preparedness in the electronic payment system was strengthened by significantly increasing the capacity for the use of BankAxept payment cards. The improvements were carried out by socially critical actors in the retail trade linked to chains with a national or regional presence as providers of groceries, medicines and fuel. The requirement to be met by the providers' merchants is that they must be able to handle seven full days of expected sales in the backup solutions. Special authorisation must still be obtained for amounts in excess of NOK 1,500. Better backup solutions reduce the importance of cash in the event of an emergency and give providers of cash services more time to obtain larger quantities of cash.

Improved security in digital channels

In 2019, the financial industry started a project through BITS that is analysing, assessing, recommending and implementing measures for the secure use of digital banking services. The purpose is to help reduce the likelihood of fraud occurring and mitigate the consequences of fraud. The project also aims to promote fraud prevention efforts and strengthen monitoring. Preventive, averting and monitoring activities of both a short and long-term nature are being considered. Many of the measures are linked to BankID and the use of digital ID, although they also include measures that supplement the use of digital ID. One of the measures involves introducing an industry standard for new unsecured credit, while other measures concern better and clearer information about BankID. Several of the measures reduce risks identified by Finanstilsynet in earlier RAV reports.

[14] Norges Bank, 3 November 2021: Norges Bank intends to enter into formal discussions with the ECB on participation in the Eurosystem's TIPS service

Public–Private Digital Cooperation (PPDC)

The public sector and the financial services industry have continued their collaboration on digitalising and improving the efficiency of important services through PPDC.[15]

The best known service, consent-based loan applications, has been adopted by more than 95 per cent of all Norwegian banks. At the same time, there are several projects in the planning or realisation phases, including within anti-money laundering. For some of the services, regulatory clarifications are needed before their full functionality can be used.

Several of the solutions are based on existing infrastructure and solutions under either public or private control. The goal is for the services to provide significant efficiency improvements and cost savings. The experience from several of the projects is that the cross-sectoral exchange of data presents regulatory challenges that need to be addressed. Both the original purpose behind collecting the data and sector-specific regulations can provide guidance on further sharing of information.

[15] BITS's website: Digital Samhandling Offentlig Privat and Aktivitetsrapport DSOP 2021 (both in Norwegian only)

3 FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS

3.1 The financial infrastructure is robust

Finanstilsynet believes Norway's financial infrastructure is robust. There were no major ICT incidents that impacted financial stability in 2021. The institutions' operational stability was satisfactory and better than in previous years.

Significantly more incidents were reported in 2021 than in 2020. The proportion of security incidents was about on a par with 2020. Even though far more operational incidents were reported, given the duration of the incidents, the number of users affected and the time of day they occurred, Finanstilsynet's assessment is that the availability of payment and other customer services was better in 2021 than in the two preceding years.

The reliability of the clearing and settlement systems was generally good in 2021, although there were some individual incidents. The reliability of the communication with the international message network for payments and securities transfers, SWIFT[16], and the international settlement system CLS[17] was also good.

The scale of cybercrime is increasing year on year, and institutions are having to deal with a constantly evolving threat picture. So far, cybercrime has not resulted in systemic crises or had serious consequences for institutions in the Norwegian financial sector. However, some serious vulnerabilities were also found in some institutions in 2021 that could have had major consequences had they been exploited.

A cyber incident can occur without warning, collapse financial infrastructure and have far-reaching societal consequences. The institutions' work on ICT, with respect to both reducing the likelihood of non-conformances and generally improving ICT security, helps ensure stable operational solutions. This includes business continuity plans, contingency plans, recovery plans and ICT security planning.

[16] SWIFT's website: About us
[17] CLS's (Continuous Linked Settlement) website: About us. US financial institution that offers settlement services to its members in the foreign exchange market (FX)

3.2 An evolving cyberthreat picture

The threat picture is changing in the financial sector as well. It has, for instance, become difficult to distinguish between threats from organised crime and threats from foreign intelligence services, and a number of criminal environments sell services to clients that include state actors. Both the Norwegian Intelligence Service (E-tjenesten) and the Norwegian Police Security Service (PST) point out that state actors are a significant threat, including through intelligence and network operations (digital mapping and sabotage of critical infrastructure), while the Norwegian National Security Authority (NSM) points out threats such as the recruitment of insiders in institutions.

The threat posed by actors looking for security holes in widely-used software appears to be increasing. Exploitable security holes can result in information leaks and/or unauthorised changes to an institution's systems and infrastructure.

The scale of criminal attacks on financial institutions' digital systems in 2021 appears to have been on a par with that in 2020. At the same time, institutions continue to work on enhancing their systems for monitoring abnormal activity, automatically managing detected incidents and averting attacks. Cyberattacks are usually averted before institutions and their customers suffer any consequences.

Institutions are constantly working to improve their expertise in cybersecurity. As described in section 2.3, good cooperation in the financial sector via NFCERT[7] is helping to improve knowledge about the relevant threat and risk picture, and better equip institutions to handle cyberthreats and prevent adverse incidents.

The institutions must continue their work on analysing risks and vulnerabilities, implementing preventive measures, and preparing to deal with attacks and the consequences of such attacks. Protecting confidential information and raising the awareness of their employees are important elements of this work.

Finanstilsynet continues to observe major differences in the maturity of institutions when it comes to assessing the risk of inadequate data protection. For the sake of prevention, it is important that institutions analyse which assets may be exposed.

3.2.1 Organised crime as a threat factor

Organised cybercrime usually has a financial objective. In other words, the criminals go for targets that could provide the greatest possible gain at the lowest possible cost. So-called ransomware is a typical method.

The organisation of the attacks has evolved, with greater specialisation and cooperation between different groupings. Services provided by criminal actors include information gathering, selling information about cyber vulnerabilities, phishing campaigns and expertise in penetrating institutions'

digital protection mechanisms. The use of ransomware[18] is becoming increasingly common among criminal organisations but has so far not had major consequences for institutions in the financial sector. It is likely that such groupings will attempt increasingly sophisticated attacks, which makes ever greater demands on the cyber defences of institutions in the financial sector in Norway.

Finanstilsynet believes that organised cybercrime will continue to represent a significant threat to Norwegian financial institutions.

3.2.2 Foreign states as threat factors

Foreign states have a lot of resources that can be used for cyberattacks. The NSM believes that threats to the financial sector could originate from Russia, China and others. The NSM regularly publishes updated risk and threat assessments, including attacks by state actors.[19]

No increase in unwanted cyber activity against Norwegian institutions in the financial sector has been observed since the start of the war in Ukraine. Nevertheless, the risk is deemed elevated, especially if the conflict escalates further or is prolonged. The situation requires enhanced monitoring and increased emergency preparedness, and institutions in the financial sector need to review their emergency response plans and capacity. It is particularly important to remove passive and outdated systems and components that are not in use, implement security updates, and verify that one's systems are free of corrupted code.

It has been revealed that Ukrainian IT systems were corrupted with malicious code long before the war in Ukraine was started.[20] These experiences underline the importance of institutions focusing on preventing unauthorised persons getting into an institution's systems and introducing malicious code even before a conflict or situation arises. The lessons learned from the war in Ukraine should be included in institutions' risk assessments.

3.2.3 Attacks on value chains

Financial services are often characterised by deliveries from different service providers and subcontractors in addition to links between actors. The utilisation of such digital value chains by cybercriminals has increased recently and the threat level for this type of attack is expected to rise. Such attacks can be carried out, for example, by cybercriminals introducing security holes into a compromised subcontractor's code. The corrupted code is then distributed further along the value chain and can result in a large number of institutions ending up with a security hole in their IT systems, which a threat actor can then exploit at a later date.

[18] See, for example, the blog dated 16 May 2021 on Dataequipment's website: NSM informer om økning i løsepengevirus (in Norwegian only)
[19] Norwegian National Security Authority (NSM) – topic page: National Cyber Security Centre (NCSC)
[20] Digi.no – article 24 February 2022: Skadevare viser at angrepet på Ukraina har vært forberedt i flere måneder, mener cybersikkerhetsselskap (in Norwegian only)

Known examples of value chain attacks are SolarWinds in 2020, Microsoft Exchange Server in 2021 and Apache Log4j in 2021, all of which hit large organisations on several continents, and the Kaseya attack in 2020, which forced several hundred Swedish shops to close temporarily.

Value chain attacks can be difficult to detect for a number of reasons. Digital value chains are often complex and can cross national borders and involve various national authorities. Growing outsourcing and the increased use of components in complex solutions make it harder to maintain oversight of what systems contain. Recognised good practice involves keeping systems updated to reduce the risk of cyberattacks. It can be challenging for institutions to find a balance between updating their systems as soon as possible with software patches and changes from service providers and performing adequate testing of software updates and changes before they are deployed in a production environment.

Measures that should be considered to counter attacks on value chains:

- Microsegmentation[21] and encryption of internal networks to prevent unwanted access and spreading of code.
- Monitoring network traffic aimed at detecting abnormal data traffic patterns or behaviour.
- Strengthening control of system deliveries, service providers and service providers' use of subcontractors, including outsourcing that includes general IT dependencies.

3.2.4 Attacks on key service providers and data centres

A significant proportion of ICT operations, in the financial sector, are outsourced to a relatively small number of key service providers and data centres, which often also provide important services to other sectors. If a key service provider experienses problems, it can cause ripple effects that impact large parts of the financial system and other important social functions in Norway. These actors can therefore be attractive targets for an attacker. At the same time, key service providers may have more resources and expertise to develop resilient solutions and the necessary emergency preparedness than institutions would individually. Using service providers can thus also help reduce the risk of cyber-attacks resulting in serious incidents in the financial sector.

Institutions should monitor dependencies on key third parties, such as operations centres, service providers, including outsourcing, and other institutions and organisations with which they cooperate, and assess the vulnerability that would result from successful attacks against them.

Institutions should also carry out realistic emergency preparedness exercises where the scenario involves the loss of one or more of the third parties identified in the vulnerability analysis discussed above.

[21] Microsegmentation involves dividing up a network, data centre and cloud implementations into segments in order to establish security controls and protect them individually.

3.2.5 National measures – TIBER-NO

In autumn 2021, Norges Bank and Finanstilsynet decided to establish the TIBER-NO[22] framework for testing cybersecurity in the Norwegian financial sector. The framework is intended to contribute to financial stability by increasing the resilience to cyberattacks of entities that perform critical functions for the Norwegian banking and payment system. Several European countries, including the Netherlands, Denmark and Sweden, have introduced similar frameworks and started testing and quality assuring critical and important functions in their financial sector.

3.2.6 Measures in institutions

Each individual institution is responsible for the cybersecurity of its own systems. This also includes those parts of its operations that are outsourced. The work consists of three components: the capacity to counter attacks, the capacity to detect attacks, and having effective plans and solutions for system recovery after attacks.

Measures for countering attacks

An important measure for countering cyberattacks is ensuring that the production systems have been updated with the latest, verified and approved versions and security updates. It is also important to remove passive and outdated systems and components that are not in use. Value chain attacks can be countered by conducting risk assessments and establishing appropriate change management controls. The necessary training and skills enhancement in the area of IT security for the organisation in general and the IT security organisation in particular are also important.

Measures for detecting attacks

To detect attacks, institutions must have the necessary expertise in-house and consider using external specialist services. Surveillance tools that can detect unwanted activities are also required.

In addition, it is recommended that institutions conduct security tests based on recognised principles.

Emergency preparedness

Financial institutions must ensure that their operations can be restored after cyberattacks and have updated and tested plans for this. In addition to having plans for re-establishing systems and any lost data, they must have plans for managing an incident up to the point where systems and lost data have been restored. Institutions must also have communication plans.

Institutions should regularly carry out scenario-based emergency preparedness exercises. The lessons learned from these exercises should be reviewed systematically in order to eliminate weaknesses and deficiencies in emergency preparedness systems and procedures.

[22] Finanstilsynet's news item 21 October 2021: Norges Bank og Finanstilsynet etablerer rammeverk for testing av cybersikkerhet i finansiell sektor (TIBER-NO) (in Norwegian only)

It is also important that institutions test how quickly they can re-establish the institution's systems in different scenarios and assess the consequences any downtime could have for the institution and the institution's customers.

3.3 The Covid-19 pandemic and the war in Ukraine

Over the past couple of years, Finanstilsynet has paid a great deal of attention to risks and challenges in the financial infrastructure due to the Covid-19 pandemic and, since February this year, also due to the war in Ukraine. In addition to ordinary meetings, the Financial Infrastructure Crisis Preparedness Committee (BFI) has held several extraordinary meetings during this period to monitor key institutions in Norway's financial infrastructure and how they are ensuring stable and secure operations, in line with the committee's remit. The BFI meetings have contributed to the sharing of information on factors that could result in disruptions to the financial infrastructure or impact financial stability, as well as on measures that the institutions have taken or are planning to take in order to improve their monitoring and ensure greater emergency preparedness and response capacity in the event of incidents. Key topics include the consequences of changes in the geopolitical landscape and cyberthreat picture, including the dependence on deliveries from countries that are at war, and approved sanctions, including the exclusion of several Russian banks from the SWIFT network.[16]

Experience shows that the key institutions in Norway's financial infrastructure have contingency plans that can be implemented rapidly. The institutions and their service providers have shown that they maintain oversight of the operational situation and have established measures.

Finanstilsynet and BFI pay particular attention to entities that support critical functions in the financial sector, including those defined as critical by the Norwegian Directorate for Civil Protection (DSB). These functions include the ability to:

i. maintain secure transfers of capital in the financial markets between national entities and to and from abroad
ii. execute payments and other financial transactions securely
iii. maintain the public's access to the necessary means of payment

The National Cyber Security Centre (NCSC) has established a forum for sectoral response environments (SRE Forum[7]). Finanstilsynet has, together with NFCERT[2], accounted for the work in the financial sector and its assessments of the consequences for the sector of the security situation due to the war in Ukraine.

3.4 Supervision of ICT and payment services

In 2021, 21 inspections were conducted in which ICT and payment services were the themes; these covered nine banks, three payment companies, two insurance companies, one investment firm, one

infrastructure company, three debt information undertakings, and two audit firms. Most of the inspections were conducted digitally because of the Covid-19 pandemic. In addition to the inspection themes specifically discussed below, Finanstilsynet also inspected account servicing payment service provider interfaces for third parties in line with the Payment Services Directive (PSD2) and the three lines of defence in the management and control of institutions' ICT systems. Furthermore, an anti-money laundering-focused thematic inspection was conducted at several banks in which systems for the electronic surveillance of suspicious transactions were the main theme of the inspection.

More details of the conducted inspections can be found on the topic page on Finanstilsynet's website.[23]

3.4.1 Business continuity and contingency plans

The inspections conducted in 2021 revealed that many institutions lack a business impact analysis (BIA) as a basis for their contingency plans. Such an analysis is important with respect to how well business continuity and contingency plans will work and for optimising crisis solutions. Contingency plans must be adequately tested and verified so that one knows that they will function in a crisis. For banks in a group, it is important that the individual bank sets requirements for being more involved in the test planning. The individual bank must ensure that it has insight into the testing and that the areas the bank has characterised as critical are adequately tested. Infrastructure institutions and other large institutions with critical functions in society must prepare a specific continutiy plan for the continuation of the services.

Business impact analyses

A business impact analysis (BIA) is an analysis that is carried out to map the effects an incident may have on an institution's business processes and services. Such an analysis is based on mapping and assessing processes and services that are critical to the institution's activities. The assessment also includes mapping and classifying the activities and resources needed to deliver mission-critical processes and services. BIAs also provide a basis for an institution's business continuity and disaster recovery plans. The institution must ensure that testing and exercises, including outsourced activities, are based on the institution's BIA in order to ensure that the continuity of critical business processes and services is safeguarded in the event of an undesirable incident. The institution should establish procedures for conducting business analyses to ensure that the continuity of business-critical services and processes is safeguarded.

Guidelines on ICT and security risk management issued by the European Banking Authority (EBA)[24] and guidelines on information and communication technology security and governance issued by the European Insurance and Occupational Pensions Authority (EIOPA)[25] both state that institutions should prepare a BIA.

[23] Finanstilsynet: Tilsynsrapporter for IT og betalingstjenester (in Norwegian only)
[24] EBA: Guidelines on ICT and security risk management
[25] EIOPA: Guidelines on information and communication technology security and governance

3.4.2 Documentation of the ICT infrastructure's components

At its inspections, Finanstilsynet found deficiencies in institutions' documentation of their ICT infrastructure. An updated and complete overview of the ICT infrastructure's components, including information about software and software versions, is an important part of security work. Both components operated by the institution itself and components operated by service providers are required to be documented. For the latter, the institution must ensure that the individual service provider maintains such an overview.

3.4.3 Vendor management

At several inspections in 2021, Finanstilsynet pointed out that the institution lacked documented risk assessments for the outsourcing of IT functions or procurements of new IT systems. Finanstilsynet also found that institutions had outsourcing agreements that lacked requirements that the institution be ensured a right of access to and oversight of the outsourced ICT operations.

3.4.4 Security

Access management

In 2021, the inspections revealed that many institutions lack adequate procedures for overseeing and following up service providers' access to institutions' systems and data. This is particularly serious if they also lack logging or procedures for monitoring logs. Finanstilsynet expects institutions to maintain oversight of the access rights employees of service providers have and be able to document these, including privileged access rights and access to sensitive data. Finanstilsynet also recommends increased use of role-based access rights, whereby access is granted based on a predefined role with rights.

After inspections in 2021, Finanstilsynet pointed out that local administrator rights should not be granted on an institution's workstations. Such rights make the institution's systems portfolio more accessible and therefore more exposed to adverse incidents and cyberattacks. Only employees in an institution's IT department should have such administrator rights.

Security tests

Institutions are increasingly making use of security testing. Testing is important for detecting vulnerabilities in applications, networks, and architecture. However, security testing may result in situations where the provider of the tests or employees of the institution gain unauthorised access to sensitive information, and adverse incidents may occur that affect the security and stability of the systems. Finanstilsynet observed through its supervisory activities in 2021 that several institutions lack guidelines for carrying out security testing. Such guidelines should, for instance, describe the risk assessments that need to be carried out in connection with testing, the frequency of testing, the conditions for selecting third party providers and how adverse incidents should be handled. The guidelines should be based on internationally recognised standards.

3.4.5 Debt information undertakings

The Debt Information Act, which came into force in autumn 2017, allows private actors to be granted a licence to establish registers for receiving and releasing debt information. The purpose of the Act is to help improve credit ratings and prevent debt problems among private individuals.

In 2021, Finanstilsynet carried out inspections of the three institutions that established debt registers in 2019. The inspections addressed the undertakings' ICT and risk management systems, focusing on measures taken to ensure that personal data do not fall into the wrong hands, and that the debt information is correct and available to relevant users. Debt information undertakings have few ICT employees and Finanstilsynet FT stressed the importance of having measures in place for keeping daily quality control documentation up-to-date and reducing the dependence on key personnel.

3.4.6 Bank mergers

Bank mergers are often demanding processes that last for a long time, often several years. The process requires a high degree of planning, testing and accuracy when making changes to and transferring data.

Bank mergers were also carried out in 2021. Finanstilsynet monitored the processes and identified some areas that require particular attention during a merger. Merging banks should have a unified testing strategy with a clear division of responsibilities. The testing of the ICT systems should be based on established acceptance criteria and cover different customer types, lending/deposits, payments, AML, collateral, archive and rights of disposal/guardianship, production of bank statements and reactivation of payment agreements related to savings agreements.

When changes are made to ICT systems, it is important to maintain high levels of emergency preparedness and call centre capacity in order to deal with any enquiries, both to reassure customers about their funds and to facilitate the early detection of any major problems that might arise.

3.5 Account servicing payment service provider PSD2 interfaces

The public law part and to some extent the private law part of the EU's revised Payment Services Directive (PSD2) was incorporated into Norwegian law on 1 April 2019. PSD2 is designed to promote innovation and competition on equal terms and through this contribute to a well-functioning market for payment services.

PSD2 defines two new types of institutions: payment initiation service providers and account information service providers, collectively called third-party providers (TPPs). Statutory provisions have been introduced to make licences mandatory for two new payment services described as so-called 'initiation services': payment initiation services and account information services, respectively. Furthermore, rules for the secure authentication of payers, third-party payment service providers and

account servicing payment service providers (ASPSPs), as well as secure communication between them, are described in Commission Delegated Regulation (EU) 2018/389 (RTS), which has been incorporated into the Regulations on Systems for Payment Services.

Several other countries' competition authorities have also been given duties related to PSD2 and have in this context been driving forces behind increasing competition in the market for payment services. For example, see the report dated 5 November 2021 from the Competition and Markets Authority om Governance of Open Banking[26].

By law, account servicing payment service providers (banks and electronic money institutions) must offer at least one interface that provides licensed institutions the right to access the customer's account after signing an agreement with the customer, see Article 30 of the Commission Delegated Regulation (EU) 2018/389[27]. Further regulations on the properties of the interface and the information included are stated in the Regulations on Payment Services and the Regulations on Payment Services Systems.

Finanstilsynet monitors that account servicing payment service providers offer interfaces in accordance with the regulations. Some banks were notified of orders for corrective measures in 2021. On a dedicated topic[28] page, Finanstilsynet provides further guidance on aspects account servicing payment service providers must address in their interfaces, including specifications and clarifications concerning the regulations. In Finanstilsynet's opinion, there are still some deficiencies in the interfaces offered by several account servicing payment service providers, which can be challenging in relation to their use by payment initiation service providers and account information service providers.

3.6 Institutions' assessments of risk and vulnerability

The institutions' assessments of risk and vulnerability are discussed below based on payment service providers' annual reporting to Finanstilsynet[29] of operational risk and security risk as well as information obtained through dialogue with a number of institutions.

[26] Competition and Markets Authority (CMA): Governance of Open Banking 5 November 2021
[27] EUR-Lex: Commission Delegated Regulation (EU) 2018/389
[28] Finanstilsynet's website: PSD2 – Presiseringer og avklaringer om regelverket (in Norwegian only)
[29] The Regulations on Payment Services Systems require payment service providers to report to Finanstilsynet, at least once a year, on the operational and security risks associated with the provider's payment services and to give an assessment of whether the measures taken by the provider are adequate. The regulations apply to banks, financial institutions, e-money institutions, payment institutions, account information service providers and branches of such institutions headquartered in another EEA state. Payment institutions with limited authorisation, cf. section 2-10(4) of the Financial Institutions Act, are specifically exempted from the scope of the regulations.

3.6.1 The institutions' assessment of important factors

In their dialogue with Finanstilsynet, institutions and providers of ICT services highlighted a number of important factors concerning ICT activities and measures implemented to mitigate risk.

Specialists in short supply

There is a great demand for ICT security specialists in information security. The institutions have said that the lack of specialists may present a challenge for areas that require cross-expertise, for example security services when using cloud services. The main challenge in recruiting information security expertise appears to be that there are fewer available resources than the market needs. Internal recruitment and training could mitigate the scarcity of specialists. Institutions stress that it seems that the specialists who are available prefer to work for institutions or groups that already have established security environments of a certain size.

Outsourcing – monitoring third parties

Institutions have strengthened their internal expertise within both purchasing and monitoring outsourced ICT services. This area has been prioritised because experience suggests that a high level of purchasing competence results in better deliveries and services from ICT service providers. Several institutions point out the importance of contact with ICT service providers on strategic, tactical and operational levels when it comes to ensuring that deliveries of ICT services meet the institutions' needs.

Institutions with a multi-service provider strategy find that the concept increases the complexity of both their technology and security. The interaction between different platforms can present compatibility challenges and often requires special ('bespoke') modifications.

Cybercrime

The institutions agree that the risk of cybercrime has increased and that the number of attack surfaces has risen. Several institutions have registered increases in the number of attacks. The institutions believe it is important to have sufficient insight into one's ICT services' security architecture. Using this knowledge to set requirements for one's own organisation and to conduct risk and vulnerability analyses helps improve general security.

The institutions point out that phishing remains the most common cybercrime method. Criminal actors are becoming increasingly professional, and institutions have observed that they are specialising in different types of threats. This has, in turn, resulted in longer value chains for threat actors. For many institutions, it is important to join networks that focus on cybercrime or to keep abreast of developments by getting insights from international and national authorities.

The institutions' use of two-factor authentication is increasing and viewed as necessary and important for ensuring that the Active Directory accounts of users/employees are not taken over by unauthorised persons or criminals logging in from locations other than the workplace's network or other secure connection (VPN).

The institutions' experiences of cybercrime indicate that sabotage can be more harmful than espionage. Ransomware is the main tool used in sabotage. The criminals' attacks are becoming increasingly sophisticated, and several incidents have been observed where the infrastructure providers' systems have been compromised.

As far as information security is concerned, the institutions believe that it is important to have good processes for keeping the ICT infrastructure updated. It is important that the various components of the ICT infrastructure are documented (for example hardware, basic software and systems) to provide an adequate overview. Good documentation is also often considered a prerequisite for completing recovery within the set timeframe after ICT incidents.

Business continuity management and crisis management

Many institutions are now choosing to have their own employees in charge of business continuity and crisis management. The business areas are more often drawn into discussions since they can best assess the impact of business disruptions. It is also important to test recovery procedures to ensure that an institution's solutions function as intended.

Access management

Institutions say that following up access management in relation to outsourced ICT services is a major challenge. This is especially true with respect to user identities with elevated access rights, for example for inspecting logs to check that use is based on the need-to-know principle. A steadily increasing number of institutions are considering basing access management on zero trust principles[30]. Access management and the use of elevated rights have traditionally been trust-based.

Management model and internal control

Through its dialogue with institutions, Finanstilsynet has learned that there is an increasing emphasis on ensuring clear divisions between the first and second line of internal control. The work on distinguishing between the first and second line is time-consuming and often requires changes in the organisation. It often takes a long time before the various roles function as intended and the second line function starts setting clear premises for the first line. This is because the expertise lies in the different units of the organisation. Based on Finanstilsynet's experience, the size of institutions is of relevance for their capacity to set up an organisation with a clear division of first and second line internal control tasks.

Data quality

The institutions are giving greater priority to ensuring good data quality. Through their day-to-day work, an institution's employees play a key role in assuring a high level of quality. The risk of errors in data weakening the basis for decision-making is greatest in the work on anti-money laundering. Data management and control have always been important tasks for institutions. However, they are

[30] In short, the zero trust principle means 'never trust, always verify'. Wikipedia.org: Zero trust security model

now considered one of the most important focus areas. In their strategies, institutions emphasise being data-driven. Experience shows that the consequences of poor data quality have become more serious.

Geopolitical factors

Institutions have focused more on assessments of country risk and other geopolitical conditions because of the war in Ukraine. Reports from both Norwegian authorities and cooperative bodies such as NFCERT show that the situation is tense and that the threat level is deemed high. Despite this, there has been little increase in activities that entail a security threat to the Norwegian financial industry. The institutions' emergency preparedness against cyberattacks was already at a high level before the conflict. The emergency preparedness level has, therefore, generally not been raised since Russia attacked Ukraine.

The institutions' assessments of the risk associated with outsourced services provided by foreign service providers, especially by ones outside the EEA, have increased in frequency and received a lot of attention from the institutions. When assessments show that the risk is higher than the institution's established risk tolerance, services have in a number of cases been brought back from abroad to service providers in Norway or the institution itself.

3.6.2 Assessments of operational risk and security risk

Finanstilsynet has collected assessments of operational risk and security risk from payment service providers[31] (institutions). For further details, please see appendix 1.

Management and control

Based on the reported material, it is evident that most institutions generally rate the risk associated with management and control as low. Apporximately half of the institutions report that the risk associated with a lack of or inadequate oversight of business-critical hardware and software, including licences, is moderate. The institutions point out that they prepare a mapping of business-critical hardware and software and keep it updated. Some use applications like Intune[32] to maintain such mapping.

[31] The deadline for submitting reports was 15 February 2022. The institutions thus submitted their responses before the war in Ukraine.
[32] Microsoft Intune is a cloud-based management tool for mobile devices that aims to provide unified endpoint management of both corporate and employees' own (BYOD) hardware in a way that protects corporate data.

Mapping of business-critical hardware, software, business functions, processes and information

To maintain control over ICT and security risks, institutions are required to systematically prepare a mapping of business-critical hardware, software, business functions, processes and information and the risks associated with them.

Guidelines on ICT and security risk management[24] issued by the European Banking Authority (EBA) and guidelines on information and communication technology security and governance[25] issued by the European Insurance and Occupational Pensions Authority (EIOPA) are important guidelines to review in the work on establishing such mapping.

The guidelines recommend that institutions establish a hardware register and an overview of functions and processes. They also state that institutions should conduct risk assessments and classify functions, processes and hardware.

For further details about the guidelines for mapping business critical hardware, software, business functions, processes and information, see appendix 5.

A significant majority of the institutions believe that the risk associated with a lack of or inadequate guidelines on security, including risk assessments of payment services, security inspections and measures for protecting users against identified risks, is moderate. Several point out that they generally have risk assessments and guidelines that are revised regularly.

Half of the institutions believe that the risk associated with adequately training and raising the awareness of employees is moderate. Several institutions report that training is emphasised, especially in relation to new employees, that security courses are arranged, and that measures aimed at raising employee awareness are carried out.

Decision support

Half of the institutions believe that the risk of deficiencies and errors in the systems increasing is moderate. Several of the institutions pointed out that BankID's transition to a new operations service provider resulted in an increase in the number of errors after the transition. Several larger institutions also pointed out that the number of errors is generally increasing due to factors such as greater complexity, major changes to solutions and others. Several payment institutions reported that inadequate or defective operational stability in the banks' PSD2 interface is impacting the operation and stability of their payment services.

Operations and emergency preparedness

A large majority of institutions consider the risk associated with new regulatory requirements to be moderate or high. New requirements often result in systems needing to be changed, and the institutions point out that this is challenging since it may require expertise that can be difficult to obtain. In

particular, the revised Payment Services Directive (PSD2), the General Data Protection Regulation (GDPR), the new Financial Contracts Act and the Anti-Money Laundering Act and Regulations have been referred to as regulations that require special attention and resources. More than half of the institutions say that the risk associated with so-called technical debt in established IT systems and the high complexity of the IT systems is moderate.

Several institutions point out that it is becoming steadily more difficult to secure access to the expertise necessary to formulate requirements for service providers and follow up deliveries. Several institutions also point to a general lack of specialists who can follow up outsourced operations. Furthermore, some institutions point out that complex system portfolios and ownership structures are contributing to increasing risk.

Several payment service providers highlight that regulatory requirements and requests for development require good adaptability and a need for the right expertise, which is increasingly more challenging to procure.

More than half of the institutions believe that the risk of the test systems not matching the production systems is moderate. Several institutions report that they are working on improving and further developing test systems. More than half of the institutions believe that the risk associated with conducting security testing before deployment is moderate. Some institutions report that they use external parties for this.

As far as risk analyses are concerned, including the identification of areas with a high risk of downtime and measures for ensuring continuous operations, more than half believe that the risk is moderate. The institutions point out that systems are tested regularly and that the risk picture varies and therefore must be assessed on an ongoing basis.

More than half of the institutions regard components that gradually wear out, or assets that gradually reach levels that require intervention, as a moderate risk. Some institutions also categorise such ‘ticking time bombs’ as high risk. Several institutions state the monitoring is performed by the operations service provider.

Several institutions highlight the threat of cyberattacks, especially ransomware, as a risk that is growing and that requires preventive measures. A more complex threat picture means that some institutions have identified a need for skills enhancement and increased resources.

Approximately half of the institutions believe that the risk associated with failing to properly train employees to handle threats and attack scenarios is moderate. The majority of the institutions have conducted security courses, and several do so on an annual basis.

Many payment service providers point out that an increasingly complex cybersecurity threat picture requires greater use of external experts in addition to the training of internal employees. Active efforts are therefore being made to raise awareness of potential threats so that they are as best equipped as possible to meet the threats they may be exposed to in a hectic work day.

Data protection

More than half of the institutions believe that the risk associated with protecting both structured and unstructured data is low, as is the risk associated with having good guidelines for classifying data. However, the rest of the institutions believe that this risk is moderate. The institutions point out that they have established guidelines and use various tools to improve security.

ID theft

Most of the institutions believe that the risk of ID theft is low. However, a small minority believe that inadequate controls that prevent unauthorised copying of payment cards (skimming) and the misuse of card details where the physical card is not present ('card not present' fraud) is associated with high or moderate risk. The institutions point out that they monitor transactions with a view to fraud and that security mechanisms that ensure customer authentication and 3D Secure have been introduced.

Internal irregularities

Approximately half of the institutions rate the risk associated with the control of internal irregularities and irregularity scenarios as moderate. The feedback indicates that the institutions are focused on these threats. Approximately half report that the risk associated with logging and notification not being adequate is moderate. Most institutions point out that they have introduced systems for monitoring, checking or spot checks, although not everyone has established special logging of activities in their systems.

It is worth noting that both the Norwegian Police Security Service (PST) and the Norwegian National Security Authority (NSM) point out that foreign state intelligence services are actively trying to recruit insiders, see section 3.2. The institutions should take account of this in their risk assessments.

Money laundering

Money laundering is an area that institutions generally rate as representing a moderate risk, although some institutions also rate it as representing a high risk. Several institutions regard the risk associated with flagging suspicious transactions with insufficient precision as moderate or high. It is pointed out that in many cases a large number of the flags are false positives. A majority of the institutions believe that the risk associated with the systems for monitoring transactions not capturing all payment transactions is moderate to high. The institutions point out that they pay a lot of attention to this area, that the systems are being further developed and improved and that external systems are procured.

A majority of the institutions believe that the risk associated with the anti-money laundering systems (AML systems) failing to adequately use data from the institutions' other systems is moderate or high. It has also been pointed out that system dependency constitutes a risk. Several institutions report that information is transferred from external systems when information is obtained and validated in connection with the establishment of customer relationships.

Several payment service providers emphasise that consumers' trading in cryptocurrencies affects the compliance risk associated with the institutions' work on anti-money laundering and counter-terrorist financing.

A majority of the institutions believe that the risk associated with the AML systems' recognition of suspicious patterns over time is moderate or high. Several institutions report that they have adopted machine learning and scenarios that use customers' earlier behaviour compared with statistical data to recognise suspicious patterns.

3.7 Risk associated with customers' use of digital services

3.7.1 Strong customer authentication

Strong customer authentication (SCA) means a solution based on the use of two or more elements that are independent of each other so that if one element is compromised it will not impact the other elements, cf. Regulations on Payment Services Systems, section 5.[33] The European Banking Authority (EBA) has published recommendations[34] that define the requirements for strong customer authentication in more detail.

Finanstilsynet is aware that the EBA's recommendations are not always followed. For example, Finanstilsynet has learned that for some cards only card details and a code to be sent as a text message to a mobile phone are required in connection with e-commerce, which according to the EBA's definition does not satisfy the requirements for SCA. A lack of compliance means that the customer is less protected against card misuse.

3.7.2 ID 'wear and tear'

BankID is important in today's digital society in order to be able to log in to various financial and non-financial services via apps and web-based solutions. The login pages of various websites and apps look quite different and there is a risk that users, over time, will not be sufficiently vigilant and critical in their use of BankID. The combination of the extensive use of BankID and variations in login contexts

[33] Regulations on Payment Services Systems
[34] EBA: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2

can result in a form of 'wear and tear' with respect to the ID and the user's caution when using it. This suggests that it should be possible to opt out of areas where the ID can be used.

3.7.3 Challenges in anti-fraud analyses

To mitigate the risk of fraud, service providers carry out follow-up checks in the form of transaction analyses and customer analyses as part of the approval of log-ins and initiated transactions. When a user uses BankID to log in to services other than online banks, the bank (BankID issuer) cannot carry out the same analyses based on transactions, i.e. analyses based on the content of the services. The issuer of BankID can still carry out some customer analyses, for example geo checks based on where and when BankID was last used.

3.7.4 Misuse of ID characteristics

Attackers use ID characteristics that are easy to get hold of in order to obtain privileges in the victim's name. One example is national identity numbers. If someone has the victim's national identity number, it is relatively simple to create a false proof of identity using the victim's name but their own photo. Thereafter, fraudsters can arrange new credit cards, mobile phone subscriptions, etc. The fraudster uses these as proof of identity, acquires new privileges in the victim's name and can, in a worst case scenario, assume the victim's identity in a number of contexts.

3.7.5 Activating blocks on credit information

To reduce the risk of fraud through the misuse of ID characteristics, the Norwegian Data Protection Authority recommends that users actively block credit ratings at credit rating agencies.[3] In order to activate such a block, the consumer must always know what agencies exist. The Norwegian Data Protection Authority maintains information about this. Users do not receive alerts about new agencies. They must stay up-to-date themselves. As far as reducing fraud based on the misuse of ID characteristics is concerned, from a consumer's standpoint it would be better if the default was for blocks to be in place for everyone and consumers themselves then had to remove such blocks when necessary. The Norwegian Data Protection Authority has taken the initiative to develop a common blocking solution via the Brønnøysund Register Centre.

3.7.6 Use of links when communicating with customers

Finanstilsynet has observed that some institutions send customers links by email or text message. Criminals use the same method when they engage in phishing via emails or smishing via text messages where they ask the recipient to click on links with the intent of either stealing information or transmitting malicious code. Finanstilsynet is aware that customers feel insecure when institutions send emails or text messages containing links that they are asked to use.

Finanstilsynet believes it is important that institutions communicate within their customers safely and securely. Rather than including links in emails or text messages, institutions should ask customers to log in to the institution's website to obtain or submit information.

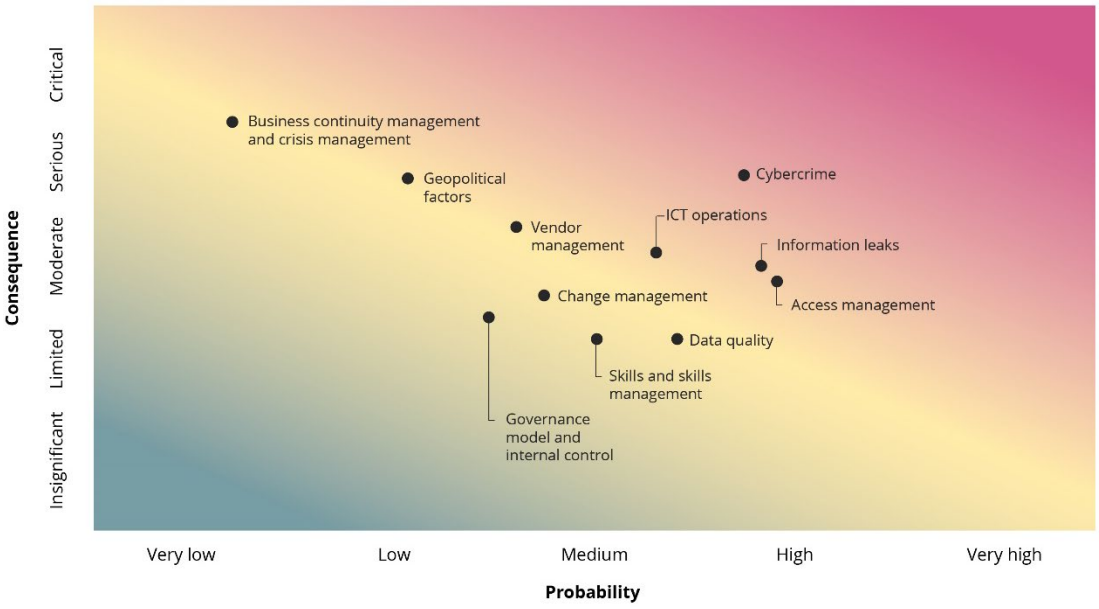
3.8 Risk associated with vulnerabilities in institutions' ICT operations

Finanstilsynet considers vulnerabilities related to institutions' defences against cybercrime to be the main risk associated with the institutions use of ICT, where the overall risk is considered high, see figure 3.1. Vulnerabilities in relation to ICT operations, access management and information leaks are also key risks, and the overall risk is considered moderate to high. While the risk associated with institutions' defences against cybercrime and access management was regarded as marginally higher in 2021 than the year before, the risk associated with ICT operations is regarded as slightly lower.

The risk associated with vulnerabilities in the institutions' business continuity and crisis management and geopolitical factors is considered moderate to high. The risk associated with vulnerabilities in the institutions' vendor management, change management, governance model and internal control, skills and skills management, as well as data quality, is considered moderate.

Figure 3.1 summarises Finanstilsynet's assessment of the main vulnerabilities in the financial sector in 2021. The various vulnerabilities are classified according to the probability of a serious negative incident occurring and the severity of the resulting consequences for the individual institution. The observations and assessments the classification is based on are provided in table 3.1 and discussed in other points in section 3 as well as in sections 4 to 6. The methodology and details on which the assessments are based are discussed in appendix 2.

Figure 3.1 Finanstilsynet's assessment of vulnerabilities and risks for 2021



Source: Finanstilsynet

Table 3.1 Vulnerabilities that could represent a risk of adverse incidents

Area	Vulnerabilities that could represent a risk of adverse incidents (Degrees of risk, probability and consequences are stated in figure 1.1)	Trend
Governance model and internal control	An inadequate overview of which controls are included in the institution's internal control and how the controls should be performed, monitored and audited may result in factors that could represent an operational risk not being identified and risk-mitigating measures in line with the institution's risk tolerance not being implemented.	→
Skills and skills management	A scarcity of resources in Norway within operations, architecture, security and new technology, as well as inadequate skills management, may lead to institutions being unable to meet current and future skills needs. Problems and errors that occur may be difficult to resolve. Dependence on foreign assistance may increase.	↗
Vendor management	Complex supply chains, with multiple service providers and subcontractors in the value chain, demanding cooperation models (strategic, administrative and operational) and a lack of expertise may result in weaker monitoring and oversight of critical and outsourced ICT services.	↗
Cybercrime	Inadequate security testing, security updating, training and awareness raising among employees, and inadequate monitoring of activities in its own technical infrastructure, including networks and systems, may result in criminals inflicting damage on the institution through cyberattacks.	↗
Information leaks	Inadequate information classification, including documentation, and controls for monitoring information that is sent by email, copied to external storage devices or copied to private cloud services may cause the institution or its customers damage if unauthorised people get their hands on the information.	↗
ICT operations	Complex integration between systems from different service providers, integration between old and new systems, multiple integration points between systems, increased functionality in self-service channels and increased use of cloud services may result in challenges in maintaining stable and secure operations.	→
Business continuity management and crisis management	Inadequate analyses of the consequences of a crisis, inadequate training and exercises in crisis management, shortcomings in disaster recovery solutions/backup solutions and inadequate backup solutions may result in challenges for institutions when it comes to maintaining critical ICT services in the event of severe disruptions at normal operating locations.	→
Geopolitical factors	Geopolitical factors or interruptions in communications with other countries, where service providers are prevented from maintaining deliveries of critical ICT services from abroad, may result in challenges in maintaining stable and secure operations.	↗
Change management	A fast pace of development, where quality is sacrificed at the expense of time, may result in functional errors in applications and systems, and security holes not being identified. Inadequate control of changes to operating configurations may result in interruptions to critical business processes and the institution being exposed to cybercrime.	↘
Access management	Inadequate control and monitoring of broader access rights, for employees and service provider personnel, may harm the institution as a result of deliberate or unconscious operational errors. It can also lead to information leaks.	↗
Data quality	Deficiencies or errors in data may result in analyses and controls being performed based on incorrect or insufficient information. This may include errors in credit ratings, errors in controls aimed at detecting money laundering or fraud, errors in risk assessments and errors in monitoring operations.	→

Source: Finanstilsynet

4 FRAUD AND FRAUD STATISTICS

4.1 Reporting of fraud statistics

According to section 2 of the Regulations on Payment Services Systems, banks, financial institutions, e-money institutions, payment institutions and branches of such institutions headquartered in another EEA state must report fraud statistics to Finanstilsynet at least once a year. Finanstilsynet has decided that the institutions' reporting on fraud should take place semi-annually, which is in line with the revised Payment Services Directive (PSD2).[35]

Both the amount defrauded and the number of fraudulent transactions are reported, as well as the total transaction amount and the total number of transactions in the period. The reporting distinguishes between domestic transactions, cross-border transactions within the EEA, and cross-border transactions outside the EEA. Furthermore, fraudulent transactions are classified into three categories based on whether the fraudster issues the payment order, changes/modifies the payment order or manipulates the payer into issuing the payment order. Fraud reporting was changed with effect from the second half of 2019 due to the introduction of PSD2, which resulted in a break in the number series.

4.2 Losses associated with the fraudulent use of payment cards

Payment card fraud is primarily fraud in which the fraudster issues the payment order. The largest subcategory is theft of card details.

Issuing banks reported that losses due to fraudulent card payments amounted to approximately NOK 159.3 million in 2021. The losses were roughly equally split between the first and second half of the year at NOK 78.5 million and NOK 80.8 million, respectively. In addition to this come losses of NOK 2.8 million through the misuse of payment cards to withdraw cash, which split between the first and second half of the year at NOK 0.8 million and NOK 1.9 million, respectively. Overall, total losses through the misuse of payment cards amounted to NOK 162.1 million. This is an increase of 9.9 per cent from 2020, but lower than the level in the second half of 2019.

Table 4.1 shows total losses from fraudulent use of payment cards owned by Norwegian customers in recent years, irrespective of whether the loss was covered by the customer, the bank or the payment card company.

[35] Article 96 no. 6 in PSD2 (EUR-Lex) and Guidelines on fraud reporting under PSD2 (EBA)

Table 4.1 Losses from fraudulent use of payment cards

Type of payment card fraud (amounts in NOK 1,000)	2016	2017	2018	2019	2020	2021
Total	206,503	145,591	148,732	189,147	147,602	162,145*

* Payments and cash withdrawals by card. Sources: Finanstilsynet and Bits AS

Total losses in 2021 stemming from fraudulent payments using payment cards amounted to 0.02 per cent of the total value of transactions. The proportion of fraud was highest for cross-border transactions outside the EEA. In this category, fraud accounted for 0.2 per cent of the value of transactions, which is lower than in 2020.

Table 4.2 Value of transactions and fraudulent transactions with payment cards reported by card issuer. Figures for 2021

Transaction value (amounts in NOK 1,000)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total transactions
Card payments (issuer)				
Total	712,504,725	211,058,563	25,467,535	949,030,823
- Of which fraud	6,277	97,722	55,356	159,355
Fraud in per cent	0.001	0.046	0.217	0.016
Of which initiated non-electronically*:				
Total	4,808,934	6,122,447	2,989,278	13,920,659
- Of which fraud	535	6,295	7,185	14,013
Fraud in per cent	0.011	0.21	0.24	0,10
Of which initiated electronically:				
Fraudster issues the payment order, of which	4,643	78,355	44,122	127,120
- Lost or stolen card	767	1,429	1,174	3,370
- Card not received	375	594	377	1,346
- Counterfeit card	29	935	1,002	1,966
- Theft of card details	2,667	51,724	35,077	89,468
- Other	806	23,675	6,491	30,972
Fraudster changes or modifies the payment order	265	571	576	1,412
Fraudster manipulates the payer into making a card payment	835	12,336	3,473	16,644
Remote payment (e-commerce)				
Total	67,787,034	138,953,771	18,857,705	225,598,510
- Of which fraud	3,869	87,340	44,794	136,003
Fraud in per cent	0.006	0.063	0.238	0.060
In-person payment (at a physical merchant)				
Total	639,908,756	65,982,346	3,620,639	102,200,353
- Of which fraud	1,875	3,921	3,377	57,355
Fraud in per cent	0.00029	0.006	0.093	0.0013
Remote payment without strong customer authentication (SCA)				
Total	27,475,944	63,050,575	11,673,834	102,200,353
- Of which fraud	1,535	27,795	28,025	57,355
Fraud in per cent	0.005	0.044	0.24	0.056

* The card transactions are initiated manually using the payment card details that were communicated verbally, via telephone, or via email. Source: Finanstilsynet

In 2021, losses from card payments that were not initiated electronically accounted for approximately NOK 14 million of the total losses of NOK 162 million from card misuse. These are card transactions in which the payment card details have been communicated by the purchaser to the seller over the telephone or via email. Measured as a proportion of the total value of transactions, the losses amounted to 0.1 per cent, while the proportion for cross-border transactions outside the EEA was 0.24 per cent. This is a decrease from 2020, when total losses from card payments that were not initiated electronically outside the EEA accounted for no less than 0.6 per cent.

The proportion of fraud is higher when using payment cards for remote purchases, typically online shopping, than for in-person shopping (using a payment card in a terminal in person at the merchant's). For payments in remote purchasing without strong customer authentication, the losses accounted for 0.06 per cent of the value of transactions in 2021, which is down from 0.07 per cent in 2020. For cross-border transactions outside the EEA, the losses amounted to 0.24 per cent, which is down from 0.35 per cent in 2020.

In total, approximately 2.5 billion payments were made by card in 2021. Of these, some 147,000 transactions were fraudulent, representing 0.006 per cent of the total number of transactions. This is a decrease compared with 2020, when the number of fraudulent transactions was 205,000 and the proportion of fraudulent transactions was 0.008 per cent.

The average value of a fraudulent transaction with a payment card was NOK 1,082, while the average value of a customer-initiated transaction with a payment card was NOK 375.

Table 4.3 Number of transactions and fraudulent transactions with payment cards reported by card issuers in 2021

Number	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total
Total	1,922,541,608	532,744,284	70,009,565	2,525,295,457
- Of which fraud	6,971	85,948	54,318	147,286
Fraud in per cent	0.0004	0.016	0.076	0.006
Not initiated electronically	9,240,296	22,415,653	21,613,880	53,269,829
- Of which fraud	392	3,961	5,423	9,776
Fraud in per cent	0.010	0.018	0.25	0.018
Remote payment	169,899,737	328,366,752	41,726,143	539,992,632
- Of which fraud	3,252	76,890	47,186	127,326
Fraud in per cent	0.002	0.023	0.113	0.024
In-person payment	1,743,401,575	181,961,879	6,669,542	1,932,032,996
- Of which fraud	3,329	5,097	1,758	10,184
Fraud in per cent	0.0002	0.003	0.026	0.00005

Source: Finanstilsynet

4.3 Losses linked to account transfers

Fraud involving account transfers includes situations where the fraudster issues or modifies the payment order or manipulates the payer to carry out the payment.

Losses due to account transfers, generally using online banks, amounted to approximately NOK 346 million in 2021, compared with NOK 355 million in 2020. The figures show total losses for online banking fraud for Norwegian customers in recent years, irrespective of whether the loss was covered by the customer or the bank.

Table 4.4 Transactions and fraudulent transactions – account transfers (online banking, etc.). 2021

Account transfers initiated electronically (amounts in NOK 1,000)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total	Fraud (%)
Total	28,889,907,250	5,692,685,875	1,142,318,500	35,724,911,625	
- Of which fraud	140,555	140,996	64,925	346,476	0.00097
Of which different types of fraud:					
- Fraudster issues the payment order	44,904	54,769	8,674	108,347	
- Fraudster modifies the payment order	5,065	8,318	277	13,660	
- Fraudster manipulates the payer into issuing the payment order	90,586	77,908	55,962	224,456	

Source: Finanstilsynet

4.4 Losses from social engineering fraud

The reported figures for social engineering fraud, i.e. where the fraudster manipulates the payer into carrying out a transaction, amounted to approximately NOK 240.6 million in 2021, NOK 224 million of which involved account transfers and NOK 16.6 million payment cards. The total losses resulting from social engineering were somewhat lower than in 2020, when they amounted to NOK 295 million, although there was a significant increase in losses where the user completed the transaction using a payment card.

The real scale of social engineering fraud is uncertain because payers must bear the financial losses themselves and many instances of fraud of this type are probably not reported to banks. Therefore, it is assumed that the actual losses are substantially higher than the reported losses. The defrauded customers often contact their bank to ask them to stop transactions and reverse the transfer of funds. Banks also alert customers when, based on their knowledge of a customer, they identify repeated transactions that are extraordinary for that customer.

Based on figures from the largest banks, Finanstilsynet is aware that the number of attempted cases of social engineering fraud is steadily increasing. The sum involved in attempted fraud (attack amount) is many times higher than the customers' actual losses. Banks are preventing a growing proportion of fraud attempts. This is probably a major reason why the reported fraud figures for 2021 are lower than in 2020. It is also assumed that greater public awareness of social engineering fraud is contributing to the fall.

Social engineering fraud still appears to be the most profitable method for criminals. The type of social engineering criminals consider the most profitable is changing. Reporting in line with PSD2's guidelines does not distinguish between various types of social engineering, although Finanstilsynet had received figures for subcategories from some of the large banks. These figures suggest that the largest category of fraud in 2021 was phishing, where the potential fraud amount was somewhat higher than before.

4.5 Losses from fraud where the fraudster issues the payment order

In the PSD2 reporting, social engineering is defined as payment transactions where the fraudster manipulates the payer into carrying out a transaction. However, phishing also includes scams where the payer is tricked into disclosing contact and payment information that the fraudster uses to issue a payment order on behalf of the payer. In PSD2 reporting, this is reported as fraud where the fraudster issues the payment order. In 2021, the losses related to transactions in online banks amounted to NOK 108 million, which is almost double the amount in 2020, while losses related to payment cards amounted to NOK 145 million.

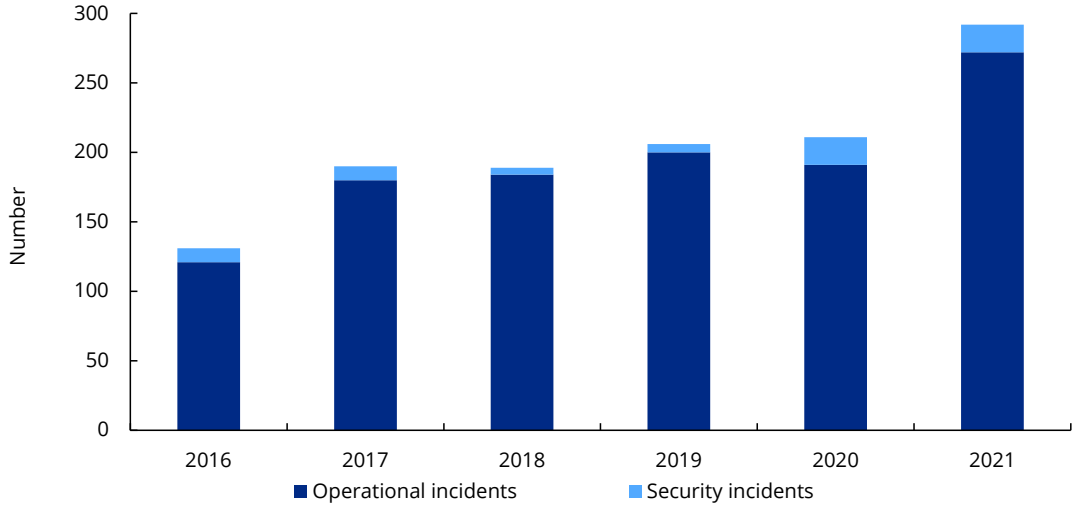
5 Incident reporting

5.1 Incident statistics

The institutions reported 292 ICT-related incidents to Finanstilsynet in 2021, which is a significantly higher number than in 2020. The increase was mainly due to more institutions reporting, such as debt collection agencies (see section 5.5), and the fact that the institutions reported more types of incidents, including incidents related to systems for detecting money laundering and terrorist financing, and to interfaces for third-party access to customer payment accounts in line with PSD2.

When incidents occur, Finanstilsynet believes that it is important that the institution identifies the causes, takes steps to prevent recurrence and prepares a final report. Incidents involving serious irregularities will be monitored throughout the duration of the incident.

Figure 5.1 Number of reported ICT incidents



Source: Finanstilsynet

Table 5.1 Number of incidents reported

Year	Operational incidents	Security incidents	**Total number of incidents**
2016	121	10	131
2017	180	10	190
2018	184	5	189
2019	200	6	206
2020	191	20	211
2021	272	20	292

Source: Finanstilsynet

5.2 Security incidents

Some 20 security incidents were reported in 2021. Many of these concerned a vulnerability in a so-called logging utility (Apache Log4j) uncovered in December 2021. The vulnerability affected operations in all sectors of society and was considered to be highly critical, since it enabled malware to be run on an infected server without having to input usernames and passwords. Institutions in the financial sector observed a number of attempts to exploit the vulnerability, although the attackers did not succeed in gaining access to the IT systems. In cooperation with their service providers, the institutions checked whether they were using the vulnerable component, made the necessary updates to their IT systems and implemented measures to monitor and handle any attempts to exploit the vulnerability. In 2022, Finanstilsynet learned that in one case attackers succeeded in infecting a server at a small financial institution with malicious code, although investigations indicated that the attackers did not have time to exploit their access before the intrusion was detected and the server taken out of service.

With respect to other reported security incidents, small financial institutions were overrepresented. The reported incidents included virus attacks on email servers and malicious code infections in text editors. Only one denial-of-service attack was reported in 2021. Several banks reported particularly aggressive phishing campaigns.

A key provider of services to the financial sector was subject to a ransomware attack in February. Institutions in the financial sector were not impacted.

Finanstilsynet communicates with NFCERT[2] when an attempt is made to exploit a vulnerability and/or the exploitation of a vulnerability is detected in widely used software that could potentially affect many institutions. Finanstilsynet published information about the vulnerability in the logging utility Log4j on its website.

5.3 Reporting vulnerabilities

In 2021, Finanstilsynet received several reports about vulnerabilities that institutions had detected in their own applications or systems. In their investigations, the institutions did not reveal attempts to exploit the vulnerabilities. If such attempts had succeeded, it could have caused serious damage, possibly with breaches of confidentiality. Vulnerabilities are most often detected by customers or employees, although they can also be detected through security testing. It is often session management problems, for example with logging out, which result in customers gaining access to another customer's data, or an account officer gaining access to other banks' data. The risk of vulnerabilities occurring is highest after changes have been made to systems.

5.4 Security breaches

In 2021, Finanstilsynet received reports from banks stating that they had detected that an ICT service provider had performed a larger number of customer searches than would appear necessary for its service provision. Investigations showed that employees at the service provider had misused their access rights. In addition to being security breaches, these also constituted breaches of the Personal Data Act and the General Data Protection Regulation (GDPR). More than 800 customers across 35 banks were affected.

This was regarded by Finanstilsynet as a serious breach of the contract between the bank and the ICT service provider. To prevent such incidents, the bank should apply the zero trust[30] principle where the use of access rights is subject to a strict regime. It is also important to document and monitor the use of access rights in relation to what is needed for work purposes.

5.5 Operational incidents

Reporting of incidents by banks and payment institutions

The most common cause of operational incidents is network problems. The risk of incidents is clearly highest after changes have been made to IT systems, and inadequate testing before solutions are deployed remain a cause of operational disruptions. With the exception of an operational incident at Danske Bank on 13 October, there were no operational incidents in 2021 of longer duration. However, there were incidents in which several banks reported recurrent instability and periodic unavailability of payment services due to operational problems at a service provider.

After Vipps changed operations service provider, Finanstilsynet considered the subsequent problems with the BankID app and code devices to be serious. Finanstilsynet held regular status meetings with Vipps and the project management in order to monitor the project progress and how the solution's stability was addressed during the transfer project. Operations were transferred in the latter part of October 2021 without major problems. Towards the end of November, problems using the BankID app arose. Finanstilsynet held frequent meetings with Vipps for a period until the operational situation was stabilised. Topics discussed at the meetings were the operational situation, relevant measures and the work on discovering the root cause.

The three main causes of the problems that arose were explained, as were the solutions that were implemented in order to stabilise BankID. The solutions proved to function as intended when traffic was restored to a normal level on 3 January 2022.

In the last few years, incidents related to changes of operations service provider have shown that in some cases the service provider had not established incident management procedures commensurate with the criticality of the service.

When changing operations service provider, the principal must quality assure that the service provider has established adequate procedures, expertise and capacity to effectively deal with incidents that impact critical services.

Reporting of incidents related to systems for detecting money laundering and terrorist financing

Banks and payment institutions reported 14 incidents of non-conformance in their electronic anti-money laundering transaction monitoring (AML systems). The reporting of incidents related to the AML systems is increasing slowly but surely year on year. The instances of non-conformance concern a lack of or inadequate screening and/or transaction monitoring. Usually the non-conformances last for shorter periods, although in 2021 Finanstilsynet also received reports of non-conformances that stretched back several years with large backlogs of transactions that had not been checked.

The most serious incidents that impact AML systems are almost exclusively caused by changes to the systems. The value chain is complex. Changes to source systems, including changing or merging source systems, impact the data retrieved from AML systems. Changes to data warehouse solutions and the relevant AML system itself also increase the risk of non-conformance. Experience underscores how important it is for institutions to test and check screening and transaction monitoring, in both the first and second line, after changes have been made. Finanstilsynet expects institutions to routinely check that the retrieval of transactions for the electronic monitoring system is complete.

Operational disruptions are often the cause of shorter periods where transactions cannot be screened and/or monitored. Finanstilsynet expects institutions to have procedures for handling situations when data transfers to the electronic monitoring system, or the electronic monitoring system itself, do not function as intended.

Reporting from the securities area

Approximately half of the incidents reported in the securities area in 2021 were related to regulated marketplaces. None of the incidents had serious consequences. However, one serious operational incident did occur in the Norwegian Central Securities Depository (Euronext Securities Oslo – ESO)[36] on 1 February 2021. The final securities settlement of the day could not be completed and was delayed until the following day.

[36] Verdipapirsentralen ASA (VPS) (Euronext Securities Oslo – ESO).

Three security incidents were reported by companies in the securities sector in 2021, all of which related to the management of global vulnerabilities, including the widely used open source code Log4j. There were no indications that criminals' attempts to exploit the vulnerabilities succeeded in damaging data or systems, also see the description in the section on security incidents. Other reports in the securities area were dominated by problems with access to online trading in securities.

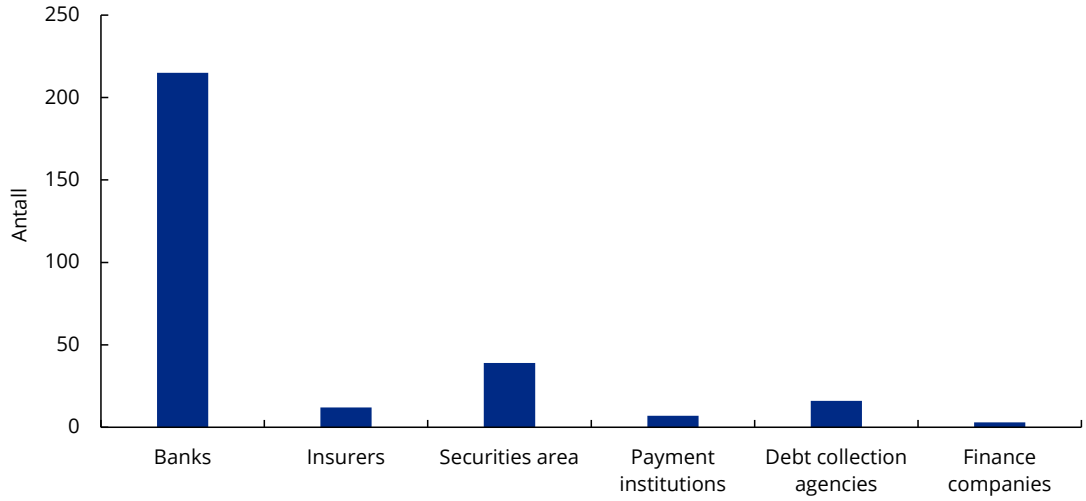
Reporting from insurers

Incidents reported by insurers were primarily incidents that impacted confidentiality or integrity and, to a lesser degree, availability. However, Finanstilsynet has observed that insurers are more often than before reporting operational incidents that affect the availability of online customer services, which are becoming a more important part of customer services. Some of the operational incidents in 2021 coincided with operational incidents at an operations service provider that serves a number of the banks. Operational incidents that impacted the insurers' self-developed systems and resulted in delays in administrative procedures were also reported. Two of the security incidents in 2021 were reported by insurers and involved different ways of compromising email accounts. One of the reported incidents involved a breach of confidentiality due to customers receiving another customer's invoice together with their own. One incident was also reported in which customers received incorrect information about the collection of tax deduction cards from the Norwegian Tax Administration.

Reporting from debt collection agencies

In a letter to the debt collection agencies in December 2020, Finanstilsynet stressed that institutions are required to report incidents in line with section 9 of the ICT Regulations. Finanstilsynet received more incident reports from debt collection agencies in 2021 than before. In 2021, several institutions, independently of each other, reported that failures in their ICT systems had resulted in dunning letters not being sent. Common to the non-conformances was that it appeared in the administrative system that the letters had been sent to the debtor and that the non-conformance was first detected by more detailed investigations resulting from a significant number of enquiries from debtors concerning letters not being received. Based on this, Finanstilsynet sent letters to all debt collection agencies where it made the institutions aware of the risk of failures in ICT systems that can result in such non-conformances.

Figure 5.2 Incidents reported in 2021 by type of institution



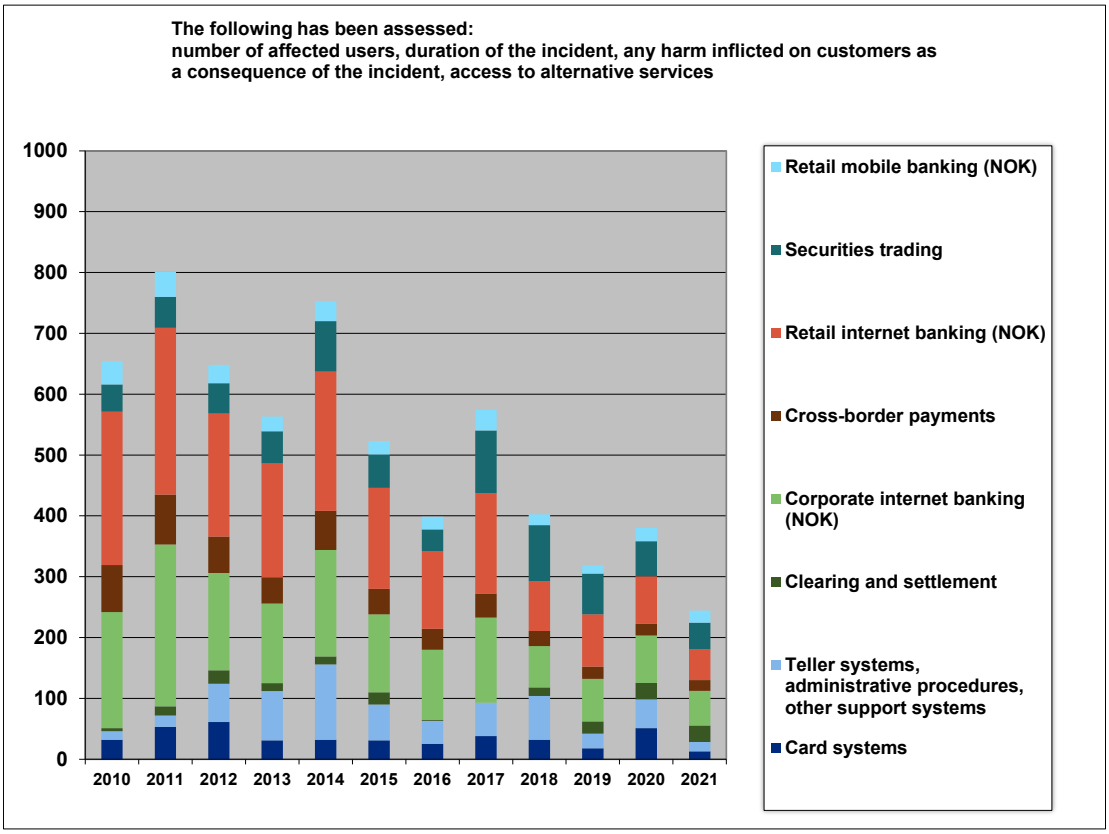
Source: Finanstilsynet

5.6 Analysis of incidents as a measure of availability

The reported incidents were of varying degrees of severity. With respect to the incidents that caused reduced availability, Finanstilsynet assessed and weighted the incidents based on when they occurred, the duration of the disruption, the number of institutions affected, the number of customers affected, and whether there were alternative services that could meet customer needs (for example when the mobile banking service is unavailable but the online bank can be used). Weighting of the incidents resulted in an index that is shown on the y-axis in figure 5.3. The findings have been collated in a time series so that the trend can be monitored over time.

Figure 5.3 shows that payment systems and other customer services were more available to customers in 2021 than in previous years. Overall, service availability was considered satisfactory in 2021.

Figure 5.3 Incidents causing reduced availability for users. Weighted by estimated impact*



*The scale on the y-axis is an index based on the weighting of each incident. A lower index value indicates fewer business disruptions with consequences for users.
Source: Finanstilsynet

There were fewer prolonged operational incidents in 2021 than in previous years, although some incidents had consequences for a large number of users.

The category 'Clearing and settlement' includes all incidents that can affect payments after the customer has approved them, such as delays, double reservations and double entries. There were a few more errors in this category than in 2020.

Incidents in the category 'Securities trading' include incidents relating to, for example, online equities trading solutions and incidents in ESO40.

The category 'Retail mobile banking (NOK)' includes apps and online mobile banks. This category is weighted up somewhat because the use of PC-based banking is falling and mobile-based banking in rising. Correspondingly, incidents in the category 'PC banking' have been weighted down somewhat.

5.7 Incidents related to problems with dedicated PSD2 interfaces

Both account servicing payment service providers and payment initiation service providers (TPPs) should according to the regulations report any problems with interfaces for third-party providers' access to customers' payment accounts to Finanstilsynet, see the account in the box below. Finanstilsynet received approximately 30 such reports from account servicing payment service providers and 13 from TPPs in 2021. Ten of these were operational incidents that were at the same time reported in accordance with section 9, second subsection of the ICT Regulations[37] on incident reporting requirements.

Duty to report non-conformance in dedicated interfaces

Payment service providers, both account servicing payment service providers and providers of the new payment services, payment initiation and account information, must immediately report issues concerning dedicated interfaces (APIs) to Finanstilsynet.[38]

Furthermore, in the event of non-conformance, account servicing payment service providers must inform third-party providers about the non-conformance and reestablishment measures and describe possible alternative solutions.

The threshold for reporting issues concerning dedicated interfaces must be lower than for incidents pursuant to the ICT Regulations.

Payment service providers must establish their own procedures for fulfilling their regulatory duties.

[37] Regulations on Use of Information and Communication Technology (ICT)
[38] Finanstilsynet on the duty to report non-conformance in dedicated interfaces: PSD 2 – Presiseringer og avklaringer om regelverket (in Norwegian only)

6 Outsourcing

6.1 Outsourcing notifications

In 2021, Finanstilsynet received more than 170 outsourcing notifications. Finanstilsynet also assessed outsourcing agreements for ICT operations when considering licence applications.

Most of the outsourcing notifications in 2021 were related to changes of service providers for the common payment infrastructure for banks, including Nets' sale of account-to-account services to Mastercard and the planned transfer of BankID's operations. In connection with the consideration of reports concerning Vipps' change of operations service provider for BankID, Finanstilsynet followed up the banks' emergency preparedness plans throughout the change period.

Finanstilsynet wishes to emphasise the importance of ensuring that the common payment infrastructure is treated as outsourced ICT services and that banks set requirements for, and follow up, the services in accordance with current regulations and their guidelines for following up outsourced ICT services.

The notifications Finanstilsynet receives are mainly of better quality and more comprehensive, detailed and complete than before. The quality of the institutions' analyses and assessments of risk prior to implementing ICT outsourcing are also showing improvements. The quality of agreements with service providers and management's understanding of the institution's outsourcing agreements also show a positive development. However, not all new institutions that apply for licences are equally familiar with the regulations.

The outsourcing notifications indicate increasing use of cloud services for both application and infrastructure services in recent years. Outsourcing means that institutions often have to deal with several platforms, for example systems at an operations service provider in combination with various cloud systems. This results in greater complexity and a more complicated risk picture. At the same time, using cloud services can also have a number of positive effects, such as better ICT security for the solutions, more functionality and services at lower cost.

Practically all institutions supervised by Finanstilsynet have entered into agreements that outsource parts of their ICT operations. Finanstilsynet provides advice[39] on what is considered outsourcing, restrictions on the right to enter into outsourcing arrangements and how supervised institutions must identify, assess and manage the risks associated with outsourcing.

[39] Finanstilsynet: Veiledning om utkontraktering (circular 7/2021) (in Norwegian only)

6.2 Regulatory changes and guidelines on outsourcing

The Regulations on the Obligation to Notify Outsourcing of Activities etc.[40] (Notification Obligation Regulations) were approved by Finanstilsynet in September 2021 and entered into force on 1 January 2022. Some factors related to the management of outsourcing are clarified in more detail in Finanstilsynet's new guidelines on outsourcing[39], circular 7/2021.

The Notification Obligation Regulations specify that the duty to notify pursuant to section 4c of the Financial Supervision Act[41] only applies to outsourcing activities that are critical or important to the institution, which constitutes a change compared to previous regulations. The Regulations also require institutions to have an updated catalogue of all outsourced agreements and notification requirements.

The provisions in the ICT Regulations[42] concerning outsourcing basically apply to all ICT outsourcing and stipulate the same processing requirements irrespective of the outsourced service's importance. The new guidelines on outsourcing lower the requirement in section 2, final subsection of the ICT Regulations that outsourcing contracts related to ICT operations and changes to such contracts shall be approved by an institution's board of directors. Section 8.1 of the guidelines allows boards to delegate responsibility for managing and making decisions about ICT outsourcing contracts not regarded as critical or important to the institution to the executive management team. Outsourcing matters that are managed by the executive management team based on delegation must be reported to the board. The provisions in section 2, final subsection of the Regulations concerning the duty to establish plans, risk assessments and descriptions of how the institution intends to control the outsourced ICT activities apply regardless of the service's importance.

Relevant guidelines on outsourcing from the EBA[43], EIOPA[44] and ESMA[45], which elaborate on the regulations, are specified in appendix 4.

6.3 Management and control

The ICT Regulations require institutions to take responsibility for all of their ICT operations, also when parts of them have been outsourced. For instance, pursuant to section 2, an institution must establish plans, risk assessments and security measures to monitor outsourced ICT services, cf. Finanstilsynet's guidelines on outsourcing[39]. Finanstilsynet expects institutions to establish management and control of outsourcing based on the principle of proportionality,[46] where the importance of the outsourced services determines the management model.

[40] Lovdata: Regulations on the Obligation to Notify Outsourcing of Activities (in Norwegian only)
[41] Act on the Supervision of Financial Institutions etc. (Financial Supervision Act)
[42] Regulations on Use of Information and Communication Technology (ICT)
[43] EBA: European Banking Authority (website)
[44] EIOPA: The European Insurance and Occupational Pensions Authority (website)
[45] ESMA: The European Securities and Markets Authority (website)
[46] Requirements for proportionality between means and ends

6.4 Risk associated with outsourcing

Security challenges

The financial industry has **long and, to some extent, complex value chains with a large number of intermediaries**. For example, one can look at banks and how they operate within the common operational infrastructure (FOI)[12] in Norway, their dependence on SWIFT[16] and the international settlement system CLS[17], as well as the requirements of the revised Payment Services Directive (PSD2)[47], where banks must provide services that ensure service providers access to data. Banks also operate complex services like consent-based loan applications.[15]

Due to the complexity and mutual dependencies, the institutions' work on reducing the likelihood of non-conformances and improving IT security is important in ensuring stable and robust operational solutions. Institutions should analyse how all parts of their service deliveries could be accessed so that they can assess the risks and opportunities that exist with respect to managing and monitoring outsourced IT services.

The institutions' **technical infrastructure** often includes local hardware, data centre solutions and cloud platforms. The various platforms, operating systems and system solutions require specialised expertise, where differences in security solutions also require specialist expertise. The security challenges associated with outsourcing increase as the overall complexity increases. In recent years, Finanstilsynet has observed that institutions are, by using cloud services, seeking to minimise the number of platforms and tools in order to reduce the need for specialist expertise. This helps reduce an institution's exposure to attacks, including alternative methods of attack, although it also entails a greater risk of concentration.

One of the most common findings from inspections of institutions' ICT activities is that they do not have satisfactory **access management** for users. This also applies to the institutions' management and control of access rights for personnel at IT service providers, who are often assigned elevated access rights so that they can perform the necessary tasks related to the outsourced IT services.

Concentration risk

Co-locating several institutions' IT operations or purchasing IT services from one or a small number of service providers can result in concentration risk. An incident that affects the service provider can have serious consequences for multiple institutions.

Norway's financial infrastructure is largely built around common solutions, including the banks' common operational infrastructure (FOI), BankID and BankAxept.

The sale of Nets' account-to-account services in 2021 resulted in several banks gaining new service providers for payment services, Mastercard Payment Services Infrastructure (MPSI) for FOI services

[47] EUR-Lex: On payment services in the internal market (PSD2)

and Mastercard Payment Services (MPS) for payment services, respectively. Several banks have also entered into contracts on card, ID and signing solutions from Nets. The sale of Nets can be seen as having reduced concentration risk, as payment services and card and ID services have been distributed between more service providers. At the same time, a large number of institutions are dependent on deliveries from MPS and MPSI, respectively, in relation to their payment services.

In 2020, Eika Gruppen entered into a contract with Tietoevry regarding delivery of core banking solutions to the local banks in the alliance. Eika Gruppen's changeover from SDC to Tietoevry will result in greater concentration risk because a large number of Norwegian banks will use Tietoevry as their operations service provider for core banking solutions.

Business continuity and emergency preparedness

The goal of establishing business continuity and contingency plans is to ensure the continuity of service deliveries in an institution. The plans are based on a business impact analysis (BIA) that identifies the institution's critical business processes. The consequences of various types of disturbances are analysed based on these processes. This includes impact analyses of how outsourced IT services would be affected by disruptions. Based on this analysis, the institution will seek to mitigate the consequences of potential disruptions by implementing risk-mitigating measures until the capacity for business continuity and emergency preparedness match the institution's risk appetite (i.e. its willingness to accept risks in relation to their consequences).

Risk management

Institutions planning to outsource IT services must be conscious of the fact that this will change their IT risk picture. For example, the IT infrastructure's potential attack surface will in most cases increase and the risks associated with IT operations will change. The ICT Regulations' provisions on risk assessments in connection with outsourcing are intended to ensure that an institution identifies the changes in risk that result from its outsourcing, and that the institution adapts to the new comprehensive IT risk picture.

Finanstilsynet's guidelines on outsourcing include recommendations on assessing service providers and formulating outsourcing agreements. The most relevant IT risks associated with IT outsourcing are listed below.

Assessments to be made when selecting a service provider (see section 5 of the guidelines on outsourcing and the ICT Regulations for further details)

The institution (principal) must:

- Assess its own capacity to manage and control outsourced IT operations. The institution must acquire sufficient expertise (section 12, final subsection of the ICT Regulations) if it lacks experience in IT outsourcing. Improving its expertise may be relevant both with respect to entering into agreements and in the management and control of the ongoing deliveries in the IT outsourcing relationship.

- Ensure that the IT service provider (contractor) has sufficient capacity, expertise and experience to perform the tasks in an appropriate manner (section 5 c) of the guidelines).
- Ensure that the contractor has established satisfactory risk management and internal control systems (section 12, final subsection of the ICT Regulations).
- Ensure that the contractor can fulfil the institution's business continuity and emergency preparedness requirements, including dealing with non-conformances in service deliveries (section 5 c) of the guidelines).
- Ensure that the risks associated with the contractor's location and the location where the tasks are performed are assessed. Examples of relevant factors include legislation/regulations, political stability, stability of the infrastructure (electricity, water, etc.), cultural differences and corruption (section 5 g) of the guidelines).
- Ensure oversight of the key person risk in the institution and at the contractor. In the institution, outsourcing services may result in reduced motivation among employees, and high turnover at the contractor can have consequences for service deliveries.

Formulation of the agreement (see section 6 of the guidelines on outsourcing for further details)
The institution (principal) must:

- Ensure that the description of the assignment clearly specifies what it involves, including quality requirements. The institution should establish plans for how it will handle poor quality and how challenges stemming from inadequate or delayed deliveries will be managed. Relevant requirements in relation to this should be incorporated into the agreement(s).
  For example, business-critical functions require service deliveries to continue even if the contractor's personnel go on strike. This must be addressed, for example through separate agreements with the trade unions/authorities (cf. section 6 b) of the guidelines and section 4 of the ICT Regulations).
- Ensure the institution's right to terminate the agreement, based on either conflict with the service provider or the institution's own strategic choices. Institutions should ensure that agreements that are entered into have exit provisions such that the service provider relationship can be terminated in a managed and controlled manner. The agreement(s) should define the parties' obligations, including the contractor's obligation to assist during the termination phase (section 6 d) and m) of the guidelines).
- Ensure that the institution and Finanstilsynet are able to supervise the contractor's performance of the outsourced services. This includes the right to supervise tasks that have been further outsourced to subcontractors, and any provisions concerning the contractor's right to change subcontractors (section 6 e), h), i), o), p) and q) of the guidelines and section 12, first and second subsections of the ICT Regulations).
- Ensure that the contractor complies with statutory provisions, such as the Financial Supervision Act, the Anti-Money Laundering Act and the Personal Data Act.
- Ensure that the contractor undertakes to perform the tasks stipulated by the institution in its business continuity and contingency plans (section 5 m) of the guidelines).

Monitoring service deliveries

In order to ensure comprehensive management and control of IT operations, the institution should establish a management model with arenas and forums for following up service providers and deliveries at a strategic (management and board), tactical (monitoring of service providers) and operational level (day-to-day monitoring of deliveries). The established management model should include representatives from the principal in all of the forums where one establishes how the cooperation and monitoring will take place. At the overarching strategic level, it is important that the institution's management and board have in-depth knowledge of the risks, challenges and alternative actions related to the institution's outsourced operations. This also applies when an institution has outsourced all of its IT operations.

In the case of outsourcing to multiple service providers (multisourcing), an institution must assess whether arenas and forums should be established in which multiple/all service providers participate.

Appendix 1: The institutions' assessment of vulnerability

Payment service providers' assessment of operational risk and security risk is summarised below, based on their annual reporting to Finanstilsynet[48]. The reporting deadline was 15 February 2022.

The summary is divided into seven topics and includes assessments from 168 institutions:

1. Governance and control
2. The value of ICT as decision support
3. Operations and emergency preparedness
4. Data protection
5. ID theft
6. Internal irregularities
7. Money laundering

The institutions are asked to assess their situation/maturity relating to each of the risks described in the form and indicate whether they assess the risk to be high, moderate or low. If the risk is assessed to be high, the institution is asked to state the reason for this. The institutions are also asked to assess whether the risk is considered to be increasing, decreasing or stable, and to provide a brief description of the measures implemented during the past year, and an assessment of whether the measures are deemed sufficient. In addition, the institutions are asked to specify which factors entail the highest risk. A further description of how to complete the questionnaire can be found below the tables.

The tables summarise the results of the survey. The institutions' responses are indicated by colour codes. Green expresses low vulnerability, yellow medium vulnerability and red high vulnerability. No colour indicates that the institution did not reply.

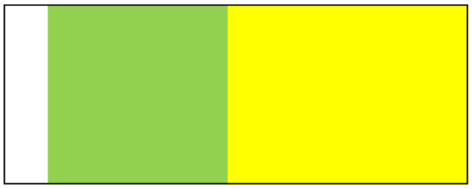
The trend, i.e. whether the vulnerabilities are considered to be increasing, stable or decreasing, is expressed in the far right column of the tables and represents the average of the institutions'

[48] The Regulations on Systems for Payment Services require payment service providers to report to Finanstilsynet, at least once a year, on the operational and security risks associated with the provider's payment services and to give an assessment of whether the measures taken by the provider are adequate. The Regulations apply to banks, financial institutions, e-money institutions, payment institutions, account information service providers and branches of such institutions headquartered in another EEA state. Payment institutions with limited authorisation, cf. section 2-10(4) of the Financial Institutions Act, are specifically exempted from the scope of the Regulation.

assessments. A horizontal arrow (where the interval is -0.2 to +0.2) indicates a stable trend. Arrows that point up indicate that vulnerability is considered to be increasing (the interval +0.2 to +1), and arrows that point down indicate that vulnerability is considered to be decreasing (the interval -0.2 to -1). For each question, an arithmetic mean of the institutions' responses is calculated.

Governance and control

Decision support

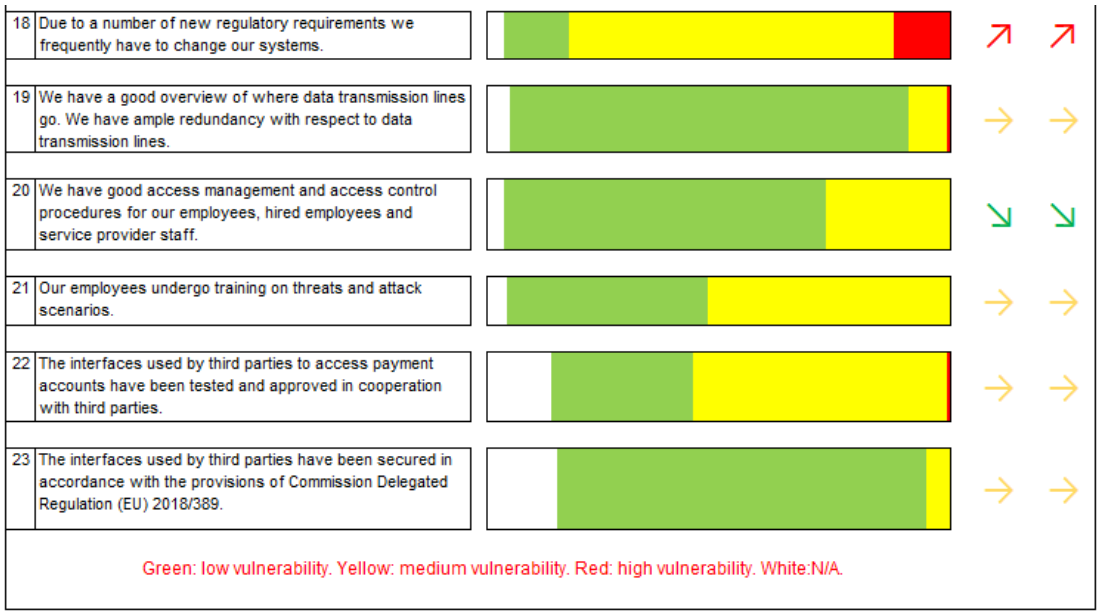
	Vulnerability	The institutions' responses	Trend 2020	Trend 2021
1	The ICT systems retrieve relevant information from external and internal sources and compile and synchronise the information into a picture of the institution's risk for the purpose of management and reporting to the authorities.		→	→
2	The ICT systems automatically provide an overall risk picture, so that if a cornerstone enterprise goes bankrupt, for example, the system automatically issues an alert about loans to the enterprise's employees and suppliers, so that we can consider writing these off as losses.		→	→
3	The ICT systems reflect customers' debt servicing capacity.		→	→
4	The information in our systems and registers is correct (data quality).		→	↘
5	Integration between the systems is automated to the extent possible.		↘	↘
6	The scope of deficiencies and errors in the systems is decreasing.		→	→
7	We collect statistical information about operations, transactions and fraud in payment services and use the information to make the services more secure.		→	→
8	We continuously consider measures to protect customers, e.g. by 1) enabling the customer to turn off features of the payment service (e.g. blocking special regions or internet access), 2) notifying the customer (by sms or email) about movements on the customer's accounts/cards or of cases where attempts to access the customer's accounts/cards are rejected, 3) giving the customer easy access to customer support.		→	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White:N/A.

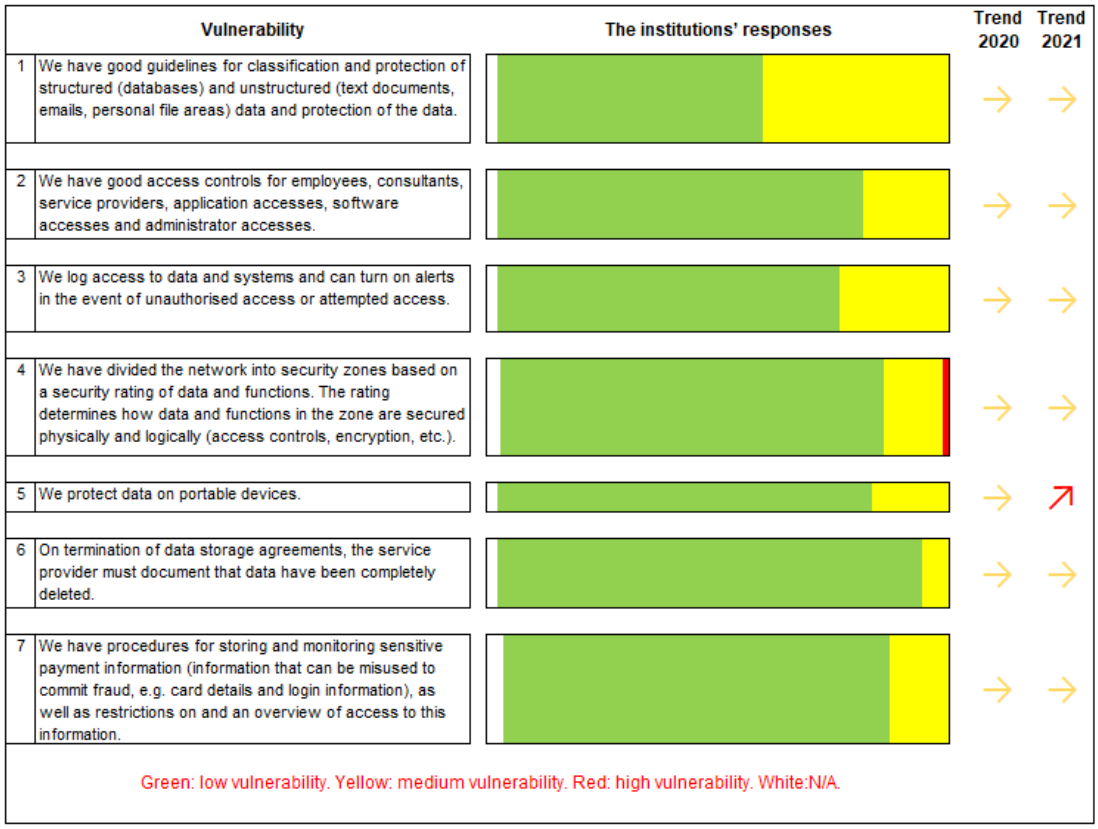
Operations and emergency preparedness

	Vulnerability	The institutions' responses	Trend 2020	Trend 2021
1	There is risk associated with non-existent or deficient procedures for change management and compliance. The root cause of errors is not uncovered and/or corrected.		→	→
2	When new IT systems are to be developed, we take the needs and systems of all departments that may be affected into account. We do this to avoid the challenges associated with 'silo solutions', such as extensive software maintenance, complicated operations and challenges associated with data synchronisation.		→	→
3	The test systems are 'production-like', i.e. test data (anonymised), applications, software, control systems and hardware are the same for testing as for production.		↘	↘

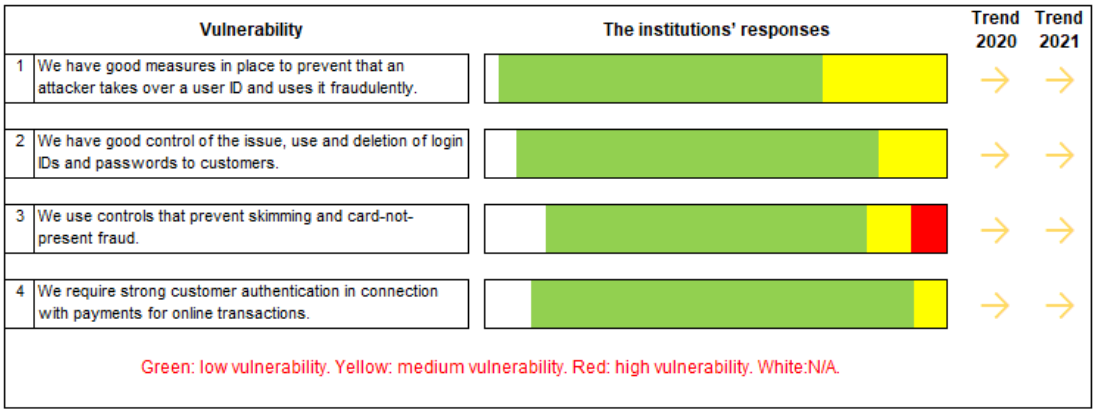
4	We make changes to the infrastructure ('non-functional' changes) during periods with little traffic and can quickly reverse the change and roll back if necessary.	→	→
5	Security tests are carried out prior to production setting. The testing is performed by persons who have not been involved in the development of the service being tested.	→	→
6	We perform regular tests to test the security of our services, (e.g. penetration testing, testing according to the TIBER standard, vulnerability scanning).	→	→
7	There is a high degree of complexity in the IT systems.	→	→
8	We implement extensive measures to protect ourselves against attacks (Advanced Persistence Threat, trojans, ransomware, DDoS, email attacks). Examples of measures: Intrusion detection and intrusion prevention, firewall, antivirus, control of web traffic, securing of email, patching and other measures to ensure stable operations.	→	→
9	We make extensive use of logging, and we have a procedure for responding quickly and adequately to 'extraordinary aspects' in the log.	→	→
10	We monitor 'ticking bombs', i.e. components that gradually wear out, or assets that gradually reach levels requiring intervention, such as memory leakage, expired certificate dates, worn out electronic components, an energy supply that is running down (batteries, fuel for emergency generator etc.)	↘	→
11	We have good measures for detecting irregularities (abnormal load, abnormal ports/protocols, irregular response times) in data traffic and take action before damage occurs.	→	→
12	We test our disaster recovery systems to an extent that makes us feel confident that they function as intended.	→	→
13	We have carried out risk analyses, identified areas with a high risk of downtime (e.g. single point of failure) and implemented measures to ensure ongoing operations.	→	↗
14	Cooperation procedures and the division of responsibilities between us and our service providers are clear-cut and detailed.	→	→
15	There is heavy pressure to deliver.	→	→
16	We have insufficient access to expertise, including the expertise to stipulate requirements for service providers and to monitor deliveries.	↗	→
17	Large 'technical debt' entails unnecessary risk with respect to change management and operations.	↘	→



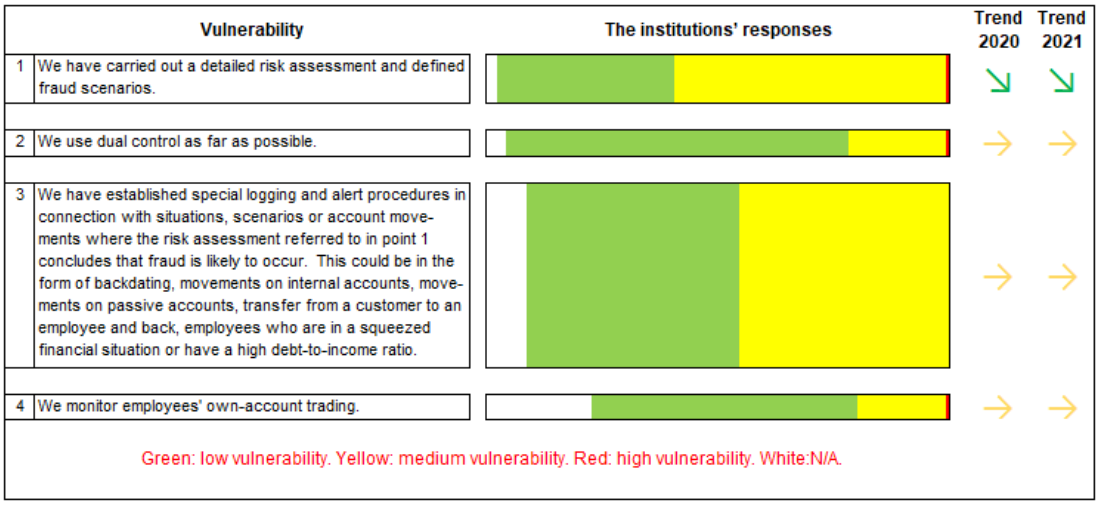
Data protection



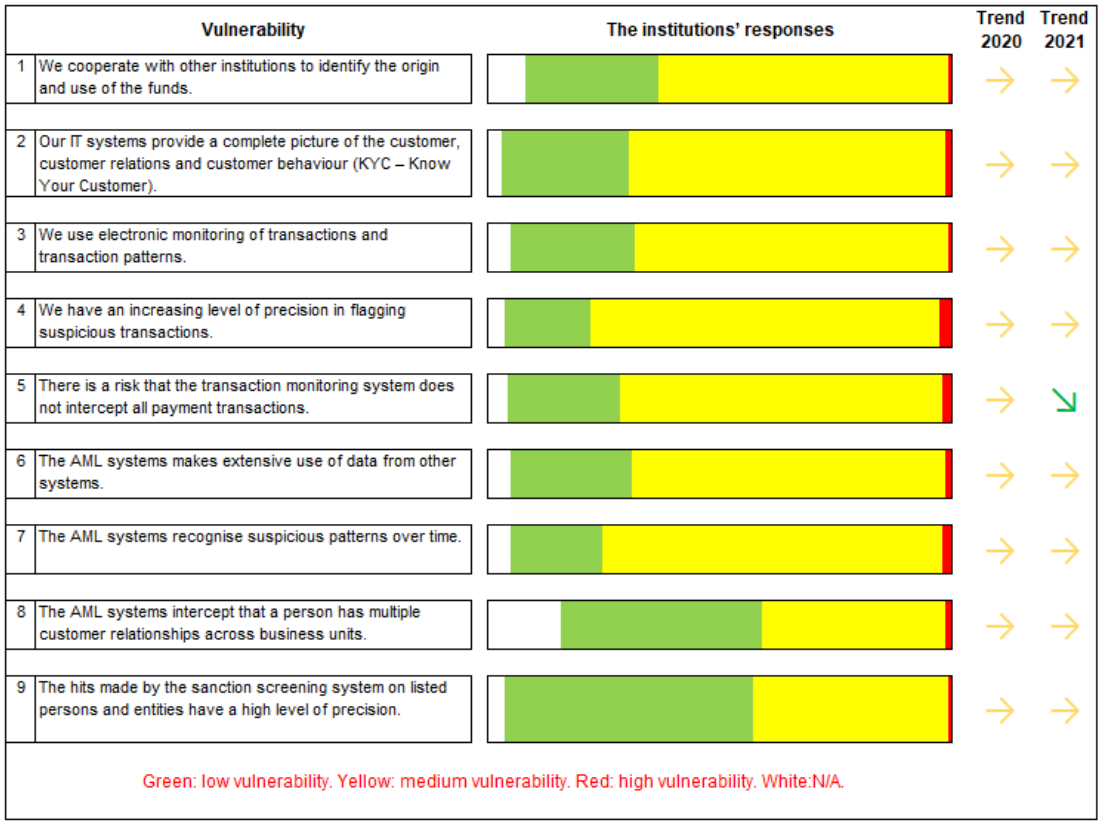
ID theft



Internal irregularities



Money laundering



Guidance to the institutions

'Finanstilsynet asks the institution to assess the risks described in the table below. The first column gives a description of the overall risk. The second column gives a description of factors that may affect the risk. The institution should assess the institution's situation/maturity and indicate in the third column whether the risk associated with the various statements is assessed to be high, moderate or low. If the risk is considered to be high, we ask the institution to state, in the fourth column, four reasons why the risk is assessed as high. In the fifth column, the institution should indicate whether the risk is considered to be increasing, decreasing or stable. In the sixth column, we ask the institution to provide a brief description of the measures implemented during the past year, and an assessment of whether the measures are deemed sufficient. If certain factors are not relevant to the institution, they should leave the cell blank or give an N/A response.

Example: The institution has experienced several incidents that have come as a surprise to the institution. It took four hours to determine the cause of the error and another two hours to correct it. The institution finds that the statement 'We have a well-established risk analysis process. Employees are familiar with the process and make active and ongoing distributions' does not give an adequate

description of the situation in the institution, which writes 'High' in the third column. Based on an analysis of the incident, the institution should state the four main reasons why the incidents occurred and why they came as a surprise to the institution, in the fourth column. In the sixth column, the institution should give a brief description of the improvement measures implemented during the past year.

Finally, the institution is asked to specify the factors that it considers to represent the highest risk, i.e. one or more risks that are particularly relevant for the institution. Please provide this information in the comment field below the tables.'

Appendix 2: Basis for the risk matrix

Finanstilsynet's assessment of risk in the different areas, classified according to probability and the seriousness of the consequences, is discussed in this attachment. Along with the observations and assessments in chapters 3 to 6, this forms the basis for the risk matrix in figure 3.1 in chapter 3.

The following definitions are used:

Vulnerability: Weakness in technical infrastructure, functions and processes that may result in undesirable incidents.
Threat: Factor with the potential to cause an undesirable incident.
Risk: Expressed as the combination of the probability of an incident and its consequences. Inadequate internal processes or systems or failure thereof, human error or external actors may increase the probability of an incident occurring, as well as its consequences.
Consequence: Results of an undesirable incident.
Risk assessment: Identification, analysis and evaluation of risk. A risk assessment lays the foundation for an institution's risk-mitigating measures and the priority given to them.

Governance model and internal control

Finanstilsynet assesses the overall risk associated with vulnerabilities in the institution's governance model and internal control as medium. The probability of the three lines of defence not revealing serious weaknesses in the institution's internal control through their activities is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of failure to comply with laws and regulations not being detected as a result of inadequate supervision by an institution's operational management is assessed as *medium* and the consequences as *serious*.
- The probability of important requirements in governing documents not being implemented and operationalised, including controls, is assessed as *medium* and the consequences as *moderate*.
- The probability of the compliance function not detecting serious weaknesses in operational units' control is assessed as *medium* and the consequences as *moderate*.
- The probability of the institution's board and executive management not possessing information that confirms or disproves compliance with internal and external requirements is assessed as *medium* and the consequences as *moderate*.
- The probability of the institution's board and executive management not having sufficient expertise and insight to help to ensure that IT investments support the institution's strategy

and needs, and lacking the necessary understanding of the risk picture to ensure stable and secure ICT operations is assessed as *medium to high* and the consequences as *moderate*.

- The probability of unclear roles in the institution's first and second lines of defence leading to serious weaknesses in the surveillance and control of the institution's governance is assessed as *medium* and the consequences as *limited to moderate*.
- The probability of serious vulnerabilities not being detected as a result of deficient risk management between operational units and the risk management function in the second line of defence is assessed as *low to medium* and the consequences as *moderate*.
- The probability of serious weaknesses in internal control not being detected by the internal audit as a result of inadequate competencies and understanding of risk on the part of the institution's internal audit is assessed as *low* and the consequences as *moderate*.
- The probability of serious organisational challenges as a result of weak change management is assessed as *medium* and the consequences as *moderate*.

Skills and skills management

At present, Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with skills and skills management as medium. The probability of adverse incidents occurring or not being adequately managed as a consequence of a lack of skills in Norway is assessed as medium and the consequences as limited to moderate. This is based on the following assessments:

- The probability of the board and the executive management not maintaining a sufficient overview of employee skills and current and future needs as a result of inadequate skills management is assessed as *low to medium* and the consequences as *limited to moderate*.
- The probability of inadequate skills management in institutions resulting in the loss of and/or an inadequate supply of the skills necessary for sound operations is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate security expertise in institutions resulting in significant operational risks is assessed as *medium to high* and the consequences as *moderate to serious*.
- The probability of business disruptions and unavailable services as a result of insufficient skills is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of breaches of information security as a result of inadequate access to security skills is assessed as *medium* and the consequences as *moderate*.
- The probability of institutions' inadequate competence in services developed and operated by service providers resulting in breaches of laws and regulations is assessed as *low to medium* and the consequences as *limited*.
- The probability of increased dependence on foreign service providers as a result of lack of resources and rising needs in Norway is assessed as *low to medium* and the consequences as *moderate*.
- The probability of inadequate understanding of the risks attending the use of cloud services resulting in adverse incidents is assessed as *medium* and the consequences as *moderate*.

- The probability of inadequate competence in new technology, such as RPA, AI and blockchain, resulting in failure to identify significant operational risks when using such technology is assessed as *medium* and the consequences as *limited to moderate*.

Vendor management

Finanstilsynet assesses the overall risk associated with vulnerabilities in vendor management as medium. The probability of adverse incidents is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of major irregularities in the service provider's internal control not being discovered by the institution is assessed as *medium to high* and the consequences as *moderate to serious.*
- The probability of security breaches occurring as a result of inadequate supervision and commitment to the security requirements by the service provider is assessed as *medium* and the consequences as *moderate*.
- The probability of an unacceptably long restoration time in the case of serious business disruptions due to unclear roles and responsibilities in the cooperation with the service provider and between service providers is assessed as *medium* and the consequences as *serious*.
- The probability of service unavailability as a result of inadequate monitoring of service quality is assessed as *low* and the consequences as *moderate*.
- The probability of undesirable dependence on service providers as a result of inadequate regulations (for example exit rules) in the agreement is assessed as *low to medium* and the consequences as *moderate*.
- The probability of undesirable dependence on service providers as a result of inadequate expertise on the part of the institution concerning the outsourced services is assessed as *medium* to *high* and the consequences as *limited to moderate*.
- The probability of inadequate (regular) risk assessments failing to detect weak sustainability on the part of service providers as a consequence of a difficult liquidity situation (bankruptcy risk), a challenging resource situation or other factors that may threaten the service provider's ability to deliver, is assessed as *low* and the consequences as *moderate*.
- The probability of serious weaknesses in a service provider's internal control not being detected through the work of a service provider's chosen auditor on an independent audit report is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate quality assurance of services acquired from different service providers and subcontractors as a result of deficient follow-up, lack of competence and failure by the service provider and subcontractors to acknowledge and comply with the institution's requirements, is assessed as *medium* and the consequences as *moderate.*

Cybercrime

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of cybercrime as high. The overall grade has not changed in this year's report, but

Finanstilsynet considers the risk to be somewhat higher than in 2021 as a result of increased criminal activity. The probability of adverse incidents is assessed as high and the consequences as *serious*. This is based on the following assessments:

- The probability of serious weaknesses in an institution's defences not being uncovered as a result of non-existent or deficient security testing is assessed as *medium to high* and the consequences as *serious*.
- The probability of an institution having serious faults in its security configuration of critical systems as a result of failure to classify its systems is assessed as *medium* and the consequences as *serious*.
- The probability of an institution having serious faults in its security configuration of cloud services is assessed as *medium* and the consequences as *serious*.
- The probability of institutions being hit by a ransom virus with loss of critical business data as a result of malware (encryption) is assessed as *medium* and the consequences as *critical*.
- The probability of an institution not detecting criminals who have established a digital foothold inside the network before damage is averted is assessed as *medium* and the consequences as *critical*.
- The probability of criminals succeeding in exploiting vulnerabilities in networks and applications before being discovered (security patch applied) is assessed as *medium* and the consequences as *serious.*
- The probability of serious security flaws not being patched in time as a consequence of inadequate security updates (patch management), including at service providers and subcontractors, is assessed as *medium* and the consequences as *serious*.
- The probability of weaknesses in defences as a consequence of the institution not being in control of the vulnerability management of software and hardware and the associated configuration is assessed as *medium* and the consequences as *serious*.
- The probability of new applications or changes in existing applications being released into production with serious security flaws, also at service providers and subcontractors, is assessed as *medium* and the consequences as *serious*.
- The probability of third-party applications integrated by a third party in or between the institution's systems and its customers resulting in adverse security incidents is assessed as *medium to high* and the consequences as *moderate to serious.*
- The probability of employees or service provider personnel representing a significant vulnerability as a result of negligence and inadequate competence in secure use of the institution's systems is assessed as *low to medium* and the consequences as *serious*.
- The probability of criminals or foreign intelligence services attempting to recruit employees or service provider personnel to gain access to information about vulnerabilities in the digital infrastructure or other information about the institution, or of the institution's employees or service provider personnel being used involuntarily, through threats, as an instrument for a cyberattack, is assessed as *medium* and the consequences as *serious*.
- The probability of employees being used involuntarily, through social engineering, as a medium for a cyberattack is assessed as *high* and the consequences as *serious*.

- The probability of disloyal employees exploiting vulnerabilities in the system for financial gain is assessed as *low* to *medium* and the consequences as *limited*.
- The probability of disloyal employees in the institution or personnel at service providers' development units planting malicious code in critical business applications is assessed as *low* and the consequences as *moderate*.
- The probability of employees or service provider personnel helping criminals to channel criminal transactions through an institution's systems is assessed as *medium* and the consequences as *serious.*
- The probability of personal data, including information about an institution's employees and service provider personnel who have roles that may be of interest to and exploited by criminals, falling into the hands of criminals is assessed as *medium to high* and the consequences as *serious.*
- The probability of institutions using methods of communication that are also used by criminals in their attempts at social engineering is assessed as *medium* and the consequences as *limited to moderate*.

Information leaks

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of information leaks as medium to high. Finanstilsynet observes that the institutions have improved their efforts to prevent information leaks and are actively working on this to safeguard their values. The probability of adverse incidents is assessed as medium to high and the consequences as moderate. This is based on the following assessments:

- The probability of classified documentation being sent from the institution in an unauthorised manner as a result of lack of classification and control is assessed as *high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control outgoing emails is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control the use of USB storage media is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control service provider personnel is assessed as *medium to high* and the consequences as *moderate.*
- The probability of confidential information that may be used to harm the institution intentionally or unintentionally being sent to or shared with external parties in an unauthorised manner is assessed as *high* and the consequences as *moderate*.
- The probability of employees or service provider personnel operating as insiders and handing over or sending confidential information, such as lists of email addresses and login information, to criminals, is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of lack of control or errors made when submitting information to customers is assessed as *medium* and the consequences as *moderate*.

- The probability of confidential information going astray as a result of use of portable equipment outside the office network is assessed as *medium* to *high* and the consequences as *moderate*.

ICT operations

Finanstilsynet assesses the overall risk associated with vulnerabilities in ICT operations as medium to high. The overall grade has not changed in this year's report, but Finanstilsynet considers the risk to be somewhat reduced compared with 2021 as a result of the improved availability of payment services and other customer services. The probability of adverse incidents is assessed as medium to high and the consequences as moderate to serious. This is based on the following assessments:

- The probability of unstable and/or unavailable services as a result of increased integration among different service providers is assessed as *medium to high* and the consequences as *moderate to serious.*
- The probability of operational problems as a result of errors in shared infrastructure is assessed as *medium to high* and the consequences as *serious*.
- The probability of operational problems as a result of inadequate competence and a lack of comprehensive understanding and overview of the institution's architecture and digital business processes is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of impaired data quality as a consequence of complex integration among service providers is assessed as *low* and the consequences as *moderate*.
- The probability of operational problems as a result of inadequate change management (hardware, applications, databases, operating systems etc.) is assessed as *low to medium* and the consequences as *moderate to serious*.
- The probability of the agreed time for correcting critical errors not being adhered to as a result of the complexity of the system portfolio, entailing integration between new and old systems, is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of monitoring of the IT environment not uncovering operational irregularities (for example expired certificates, databases, memory leaks and electronic components) is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of operational problems as a result of inadequate follow-up of technical debt is assessed as *medium* and the consequences as *moderate.*
- The probability of the test system not being sufficiently similar to the production system is assessed as *medium to high* and the consequences as *moderate to serious.*

Business continuity management and crisis management

Finanstilsynet assesses the overall risk associated with vulnerabilities in business continuity management and disaster management as medium to high. The probability of adverse incidents resulting in the activation of disaster recovery systems for critical business processes is assessed as very low to low and the consequences as serious to critical if the system does not function as intended. This is based on the following assessments:

- The probability of the institution's disaster recovery system not being established in accordance with its needs as a consequence of the absence of or inadequate business impact analyses and requirements is assessed as *medium to high* and the consequences as *critical* if the system has to be activated.
- The probability of institutions not being adequately prepared to respond to a serious situation as a result of deficient training and exercises is assessed as *medium* and the consequences as *critical*.
- The probability of the emergency response management of an institution and its service provider being inadequately coordinated in the event of a serious incident is assessed as *medium* and the consequences as *critical*.
- The probability of institutions failing to handle a serious incident effectively as a consequence of unclear roles and responsibilities internally and between the institution and the service provider is assessed as *low to medium* and the consequences as *serious*.
- The probability of the disaster recovery system not functioning as intended owing to deficiencies in the technical set-up and infrastructure and testing of the system, as well as in the evaluation of the tests, is assessed as *low to medium* and the consequences as *critical*.
- The probability of inadequate updates, including security updates, of the disaster recovery system is assessed as *low to medium* and the consequences as *serious*.
- The probability of an institution affected by a serious digital attack not being capable of handling the situation effectively as a consequence of the lack of a business continuity plan to handle cyber attacks and inadequate training and exercises is assessed as *medium* and the consequences as *critical*.

Geopolitical factors

Finanstilsynet assesses the risk associated with vulnerabilities in relation to foreign operators that deliver critical ICT services to Norwegian institutions as medium to high. Although there were major changes in geopolitical factors in 2021, partly due to the Covid-19 pandemic, the institutions have implemented measures showing that they are handling the problems caused by the pandemic in a good way. The institutions have informed Finanstilsynet that the war in Ukraine has changed the threat picture from a cybersecurity perspective, although no increase has been reported in the number of incidents. The probability of adverse incidents when foreign service providers are cut off from delivering their services is assessed as low and the consequences as serious. This is based on the following assessments:

- The probability of an institution's disaster recovery personnel being able to maintain secure and stable operations in situations where foreign service providers are unavailable, is assessed as *low* and the consequences as *serious*.
- The probability of an institution's disaster recovery personnel not being able to maintain secure and stable operations in the event of serious ICT incidents where foreign service providers are unavailable, is assessed as *low to medium* and the consequences as *serious*.

- The probability of a breakdown in communication with foreign operators, whereby the foreign provider will be cut off from performing critical ICT services, is assessed as *low* and the consequences as *serious*.
- The probability of institutions being affected by geopolitical factors related to ICT operations is assessed as *low to medium* and the consequences as *serious*.

Change management

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with change management as medium. The probability of adverse incidents is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of service unavailability as a result of non-functional changes (changes in the configuration of operating components) is assessed as *medium* and the consequences as *moderate*.
- The probability of weaknesses in change management procedures (including inadequate testing) is assessed as *medium* and the consequences as *moderate*.
- The probability of failure to establish adequate controls for identifying functional and non-functional changes that have been released into production without monitoring the change process, so-called unauthorised changes, is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of functional changes (software) introducing vulnerabilities into institutions' defences is assessed as *low to medium* and the consequences as *moderate*.
- The probability of a high rate of change due to new business functionality and regulatory requirements resulting in solutions being put into production without the necessary quality assurance is assessed as *medium* and the consequences as *moderate*.

Access management

Finanstilsynet assesses the overall risk associated with vulnerabilities in access management as medium to high. The overall grade has not changed in this year's report, but Finanstilsynet considers the risk to be somewhat higher than in 2020 as a result of reported incidents and completed inspections. The probability of adverse incidents is assessed as medium to high and the consequences as moderate. This is based on the following assessments:

- The probability of employees with extended access rights performing illegal actions is assessed as *low to medium* and the consequences as *moderate*.
- The probability of service provider personnel with extended access rights performing illegal actions is assessed as *medium* and the consequences as *serious*.
- The probability of employees or service provider personnel having access rights without the institution's executive management being aware of it is assessed as *medium to high* and the consequences as *moderate*.

- The probability of employees or service provider personnel having extended access rights without the institution's executive management being aware of it is assessed as *medium to high* and the consequences as *moderate to serious*.
- The probability of confidential information going astray as a result of inadequate access management and control of employees' accesses is assessed as *medium to high* and the consequences as *moderate*.
- The probability of confidential and/or classified information going astray as a result of a service provider's security breaches is assessed as *medium to high* and the consequences as *moderate*.
- The probability of service provider personnel, or a service provider's subcontractor's personnel, breaking rules while performing operating tasks is assessed as *medium to high* and the consequences as *serious*.

Data quality

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with data quality as medium. The probability of adverse incidents is assessed as medium and the consequences as moderate. This is based on the following assessments:

- The probability of decisions being based on the wrong premises is assessed as *medium* and the consequences as *moderate*.
- The probability of the AML system not intercepting all payment transactions is assessed as *medium to high* and the consequences as *moderate*.

Appendix 3: Finanstilsynet's monitoring activities

Finanstilsynet's supervision of ICT and payment services – key areas

Supervisory activities are risk-based, and Finanstilsynet gives priority to institutions that have the greatest influence on financial stability and well-functioning markets. ICT risk is assessed, and the institutions' own annual assessments of ICT risk are reviewed. Emphasis is placed on monitoring the organisation of ICT / cyber security work, the security of institutions' ICT systems and the organisation of surveillance activities. Inspections include institutions' control of access to systems, particularly those containing sensitive information, and the institutions' testing of possible penetration of their systems.

Other prioritised topics for supervision will be overall governance of ICT operations, emergency response work relating to business continuity and disaster recovery systems and the testing thereof, the institutions' governance, control and monitoring of outsourced ICT operations, the institutions' payment services and ICT systems for detecting money laundering and the financing of terrorism. Finanstilsynet places emphasis on the institutions having procedures in place for ensuring complete data extracts to anti-money-laundering systems. The use of new technology, major changes in the ICT area and extensive changes in the financial infrastructure are also relevant areas subject to monitoring.

Work on payment systems

The EU's revised Payment Services Directive (PSD2)[47] has been incorporated into Norwegian legislation and will form the basis for the supervision of institutions' payment services. Institutions will be monitored with respect to their compliance with the new regulations relating to payment service systems[49], risk related to payment services and compliance with the duty to report new or changes to existing payment services. Account servicing payment service providers' interfaces (APIs) for trusted third parties' account access will also be followed up, cf. opinion from the European Banking Authority (EBA)[50]. When processing concessions, care will be taken to ensure that the institutions have well-documented procedures in areas relating to ICT and payment services.

In addition, Finanstilsynet will monitor whether the institutions have robust payment solutions and have established satisfactory contingency measures for the solutions and the electronic payment system.

[49] Regulations on Payment Services Systems
[50] EBA's statement on trusted third parties' account access: EBA calls on national authorities to take supervisory actions for the removal of obstacles to account access under the Payment Services Directive

The cooperation with Norges Bank on the payment system and financial infrastructure will continue.

Follow-up of incidents

Following up ICT incidents is a prioritised part of supervisory activities. Finanstilsynet will continue to closely monitor developments in 2022. When incidents occur, emphasis will be placed on whether the institution identifies causes and takes steps to prevent recurrence. Incidents involving serious irregularities will be monitored throughout the life of the incident. Targeted measures will be considered. Vulnerabilities identified in the institutions' ICT solutions will also be followed up.

Finanstilsynet will continue to make an annual review of incident reporting of the largest institutions.

It will also be followed up that both account servicing payment service providers and third-party providers report instances of non-conformance in accordance with PSD2 and that the account servicing payment service providers correct the discrepancies and inform the third-party providers.

Outsourcing of ICT activities

Finanstilsynet will continue to monitor institutions' outsourcing of ICT activities and ensure that the institutions, when entering into a new or amended agreements on outsourcing of ICT activities that are critical or important to the institution, reports this to Finanstilsynet, as required by Section 4c of the Financial Supervision Act, cf. the Regulations on the Obligation to Notify Outsourcing of Activities[51].

Supervisory activity includes monitoring that the institutions prepare risk analyses and make a prudent assessment of the outsourcing relationship, that the agreements are in line with regulations and that the outsourcing is handled in a proper manner by the institution, cf. Section 2 of the ICT Regulations.

Contingency preparedness

The work of the Financial Infrastructure Crisis Preparedness Committee (BFI) will continue. BFI reviews incident scenarios and determines whether the responsibilities associated with crisis situations are sufficiently clear. Emergency response exercises are planned for 2022 as well, and measures linked to findings from previous exercises will be followed up.

Special incidents, such as the Covid-19 pandemic, the war in Ukraine and the institutions' organisation of their ICT activities, will be monitored, particularly at key operators in the financial infrastructure.

Finanstilsynet participates in relevant contingency preparedness work initiated by other sectors and in cooperation within the national regulatory framework for managing ICT security incidents, partly through the National Cyber Security Centre (NCSC), established by the Norwegian National Security Authority (NSM).

[51] Regulations on the Obligation to Notify Outsourcing of Activities (in Norwegian only)

Finanstilsynet will align its contingency work and handling of ICT security incidents with NSM's framework for handling ICT security incidents[52]. Finanstilsynet is the sectoral response environment (SRE) in the financial market area and exercises its role in collaboration with Nordic Financial CERT according to agreed information exchange rules. The NSM framework forms the basis for the interaction between Finanstilsynet and Nordic Financial CERT.

Monitoring of the cybercrime threat picture

Finanstilsynet will remain constantly informed of institutions' use of ICT and developments in payment services, including specific developments relating to:

- the cybercrime threat picture
- contingency preparedness work targeting digital vulnerability and security
- institutions' organisation and follow-up of security work
- changes in payment services due to the use of new technology (fintech)
- cross-border activities

In 2021, Finanstilsynet and Norges Banks estabished a framework for cybersecurity testing in the financial sector (TIBER-NO), thus aiming to promote financial stability by increasing the resilience of critical functions in the Norwegian financial sector against cyberattacks. The project will be followed up by a steering group chaired by Norges Bank with participants from Finanstilsynet.

Finanstilsynet will hold regular meetings with institutions and Nordic Financial CERT and participate in the Norwegian Cyber Security Centre (NCSC), the European supervisory authorities' work on ICT security and the European Systemic Cyber Group (ESCG) under the European Systemic Risk Board (ESRB).

Consumer protection

Finanstilsynet will control that institutions establish digital solutions in compliance with the regulations, and that the solutions launched have built-in security and functionality in line with consumer expectations. Emphasis will also be placed on whether the institutions ensure that use of their solutions and services is secure for customers.

In addition, Finanstilsynet will monitor that institutions do not share customer data without consent, and that data do not fall into the hands of unauthorised third parties. Finanstilsynet will also control that the institutions communicate with their customers in a safe and proper manner, which includes not sending or requesting information about the customer or the customer's exposures by email or making customers feel unsure by attaching links in emails or SMS communication.

[52] Norwegian National Security Authority: Rammeverk for håndtering av IKT-hendelser (Framework for handling ICT incidents) (in Norwegian only)

Payment service systems will be controlled to ensure that they do not require users to accept additional functionality in order to be able to use the service, and that users are given the opportunity to protect themselves against adverse incidents, such as the ability to block their cards against online use.

Based on new requirements for reporting fraud relating to the use of payment services, cf. Section 2 of the Regulations on Payment Services Systems, Finanstilsynet will examine the total extent of fraud and, when needed, also individual operators.

If incidents occur, Finanstilsynet will follow up that the institutions provide customers with information on how they become affected and how the institution or customers themselves can mitigate the situation.

Finanstilsynet will continue to follow up that banks discharge their responsibilities with respect to compliance with the provisions of the Financial Institutions Act[53] regarding cash services. Finanstilsynet will also control that banks have established solutions in line with the provisions of the Financial Institutions Regulations regarding solutions to meet increased demand for cash in a crisis situation[54].

[53] Act on Financial Institutions and Financial Groups (Financial Institutions Act)
[54] Regulations on Financial Institutions and Financial Groups (Financial Institutions Regulations)

Appendix 4: Guidelines from EBA, EIOPA and ESMA

Relevant guidelines concerning outsourcing from the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) that elaborate on the regulations.

EBA:	
EBA/GL/2021/05	Guidelines on internal governance under Directive 2013/36/EU EBA
EBA/GL/2019/02	Guidelines on outsourcing arrangements
EBA/GL/2019/04	Guidelines on ICT and security risk management
EIOPA:	
EIOPA-BoS-14/253	Guidelines on system of governance
EIOPA-BoS-20-002	Guidelines on outsourcing to cloud service providers
EIOPA-BoS-20/600	Guidelines on information and communication technology security and governance
ESMA:	
ESMA50-157-2403	Guidelines on outsourcing to cloud service providers

Appendix 5: Mapping of business-critical assets, software, business functions, processes and information

As a consequence of recent years' technical developments, institutions in the financial sector increasingly have interlinked/complex ICT services, several platforms (on-premises, traditional data centre and cloud services) and multi-sourcing arrangements (several service providers who in turn may have subcontractors). This results in a more complex risk picture and a larger attack surface for malicious activity. In order to be able to manage ICT and security risk, these developments require the institutions to take a more systematic approach to mapping critical processes, software, assets and information and the associated risks.

According to the two guidelines from the European supervisory authorities focusing on ICT, the institutions should maintain such mapping:

EBA: Guidelines on ICT and security risk management[55] (EBA GL)
EIOPA: Guidelines on information and communication technology security and governance[56] (EIOPA GL)

Finanstilsynet emphasises that the guidelines for establishing the various mappings describe the desired outcome. The institution determines the number of mappings and systems to be included.

Asset inventory

The institution should maintain an up-to-date inventory of its IT assets (asset inventory) (EBA GL, guideline 50 and EIOPA GL, guideline 44.). The asset inventory should include IT systems, network devices, databases, etc. In addition, the asset inventory should be sufficiently detailed to enable the institution to promptly identify assets, their location, security classification and ownership (EBA GL, guideline 53 and EIOPA GL, guideline 44). The asset inventory should also document the configuration of the assets and the links and interdependencies between the different assets (EBA GL, guideline 53 and EIOPA GL, guidelines 31 and 45).

[55] EBA Guidelines on ICT and security risk management
[56] Guidelines fon information and communication technology security and governance

Mapping of functions and processes

The institution should establish and maintain an updated mapping of their **business functions, roles and supporting processes, documenting the functions/processes** by including information about data processed, IT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes. At a minimum, the institution should register and document critical business functions and processes (EBA GL, guidelines 15 and 16 and EIOPA GL, guideline 17).

Risk assessment and classification of functions, processes and assets

Assets, business functions and supporting processes should be classified according to criticality, where the classification, at a minimum, should consider protection requirements of confidentiality, integrity and availability (EBA GL, guidelines 17, 18 and 19 and EIOPA GL, guideline 17). Data/information must be processed and stored in accordance with the classification.

The institution should **identify and document ICT and security risks** that may affect their assets, business functions and supporting processes, and ensure that risks are reassessed on a periodic basis and ahead of major changes affecting assets, business functions and processes (EBA GL, guideline 20 and EIOPA GL, guideline 17).

The classification of and information about business functions and supporting processes should be reconsidered/updated when performing periodic risk assessments and major changes affecting assets, business functions and processes (EBA GL guidelines 17, 18 and 53 and EIOPA GL, guideline 17).

Practical use of the mappings

The mappings are, for instance, important for:

- Business Impact Analyses
- management and control of business continuity processes
- the development of response and recovery plans, where documentation of the interdependencies between assets can be used, for example, in following up security and operational incidents, including cyberattacks.
- the work on configuration and change management
- protection of information to prevent data from going astray
- proritisation of remedial actions as part of vulnerability management (most important assets first) – important to keep track of the latest software versions
- life cycle management of hardware and software to control decommissioned assets and services that are no longer supported

FINANSTILSYNET
Revierstredet 3
P.O. Box 1187 Sentrum
NO-0107 Oslo

Tel. + 47 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

05.2022